УДК 519.72

DOI: 10.18664/ikszt.v0i3.140329

БОЙНІК А. Б., доктор технічних наук, професор,
БУТЕНКО В. М., кандидат технічних наук, доцент,
ГОЛОВКО О. В., кандидат технічних наук, доцент,
УШАКОВ М. В., старш. викладач (Український державний університет залізничного транспорту)

Оптимізація алгоритму субекспоненціальної складності для розв'язання SAT задачі

При модернізації і створенні сучасних систем управління на залізничному транспорті створюються оптоелектронні аналоги електромагнітних реле. При їх побудові виникає необхідність розв'язання в реальному часі задачі здійсненності бу́левих фо́рмул (SAT задача). В даній роботі для SAT задачі запропоновано алгоритм субекспоненціальної складності, який визначає, чи здійсненна функція, а також процедура, що дозволяє перерахувати всі набори змінних, на яких булева функція здійсненна за субекспоненціальний час.
Ключові слова: *SAT задача, булева функція, субекспоненціальна складність.*

Вступ

З часу стрімкого створення сучасних систем управління на залізничному транспорті [1] й до сьогодні створюються нові, сучасні оптоелектронні аналоги електромагнітних реле [2]. Застосування мікроелектронних компонентів в інформаційно-вимірювальних системах [3] дозволило оптимізувати моделі та систему обліку електроенергії за критерієм точності, що призвело до суттєвого заощаджування коштів. В роботі [4] розглянуто аспекти математичного моделювання в розподілених інформаційно-керуючих системах залізничного транспорту. Результати теоретичних досліджень пошуку найбільшої кліки на прикладі оптимізації розподілених інформаційних систем залізничного транспорту досліджено в роботі [5] й запропоновано процедуру такого пошуку в системах, поданих неорієнтованим графом.

Моделі потоку сигналу та альтернативну формулу виграшу для мультиметра мікрохвильового випромінювання наведено в [6], а їх реалізація базується на функціях алгебри-логіки. Компоненти розподілених інформаційно – вимірювальних або інформаційно-керуючих систем вдало використовуються для оптимізації обліку електроенергії на комерційних точках обліку [7].

Аналіз досліджень

Однак недостатньо приділено уваги розв'язанню задачі здійсненності бу́левих фо́рмул (SAT), хоча в зазначених системах, на низовому рівні, застосовуються булеві функції алгебри-логіки. SAT - це проблема визначення можливості розв'язання булевої формули. Формула називається розв'язуваною, якщо для неї існує набір змінних, що виконує її, тобто набір значень всіх змінних, що входять у формулу, на яких формула істинна. У російськомовному варіанті вона відома як задача «выполнимость» (ВЫП).

Ця задача має важливе прикладне значення: при верифікації програмного і технічного забезпечення сучасних інформаційно-керуючих та інформаційно-вимірювальних систем, у тому числі на ПЛІС [8-12], при розв'язанні задач автоматизації доказів, пов'язаних з перевіркою суперечливості множини диз'юнктів у обчисленні висловлювань. SAT задача знаходить так само широке застосування в задачах про кореляцію [13]. Для реалізації вимірювання параметрів сигналів і трактів НВЧ [14] теж можливе застосування множини булевих функцій. Алгоритми шифрування теж можна розглядати в термінах КНФ (кон'юнктивна нормальна форма) й інтерпретувати задачу криптографічного аналізу, як задачу знаходження вирішального набору, де вирішальним набором є секретний ключ.

Отже, задача SAT має важливе значення в системах автоматичної перевірки доказів, де формулою називають набір клозів (clause), під якими розуміється диз'юнкція деякої кількості літералів - змінних X і $\overline{X}$. Велике значення дана задача має при з'ясуванні здійсненності схем CIRCUIT-SAT (circuit-satisfiability problem). Відомо багато експоненційних

алгоритмів їх розв'язання і евристичних підходів поліноміальної складності. Серед них слід відзначити алгоритм Моніена і Шпікермайєра 1985 р., в якому для задачі *3-SAT* використовується простий перебір: по черзі пробується підстановка замість кожної змінної 1 або 0 і потім рекурсивно розв'язується задача меншого розміру, він має часову складність $\boldsymbol{O}(1{,}84^n)$. У загальному випадку можна виділити два основних типи алгоритмів для розв'язання SAT задач: алгоритми локального пошуку, які починають з якогось набору значень (він, звичайно, не виконує всю формулу), а потім модифікують його, намагаючись послідовно наблизитися до виконуваного набору, і так звані *DPLL*-алгоритми (за іменами творців, Davis, Putnam, Logemann, Loveland; їх опис базових принципів роботи цього методу відноситься до 1968 р.), які обходять дерево будь-яких наборів і виконують пошук в глибину. Процес локального пошуку, як правило, має імовірнісний характер - адже потрібно почати з якогось набору, який інакше як випадково вибрати важко, а від нього може залежати дуже багато. Слід зазначити, що DPLL-подібні алгоритми більш детерміновані, багато в чому завдяки розвиненій Олівером Кульманом (Oliver Kullmann) і Хорстом Люкхардтом (Horst Luckhardt) теорії, що зв'язує ці оцінки з розв'язанням рекурентних рівнянь. Їх ідея виявилася настільки плідною, що дозволила навіть створити програми, які автоматично доводять нові верхні оцінки складності для заснованих на цих принципах алгоритмів. Таким чином, алгоритми, засновані на локальному пошуку, виграють практично, а DPLL-подібні алгоритми – теоретично, для них вдається довести сильніші верхні оцінки. Розміри задач, що розв'язуються зараз промисловими серверами , обчислюються сотнями і тисячами змінних, що вже свідчить про високу ефективність, адже базовий алгоритм у них все одно експоненціальний. Розмірності задачі SAT, які виникають при використанні сучасних технологій розробки ПЛІС, ростуть дуже швидко, тому буде актуальною розробка ефективних алгоритмів розв'язання SAT задачі, тобто алгоритмів з малою часовою складністю, що завжди дозволяють відповісти на питання: чи здійсненна булева функція і, якщо вона здійсненна, вказати набір змінних, на якому вона здійсненна.

Мета дослідження

Всі відомі детерміновані алгоритми розв'язання SAT задачі мають експоненціальну складність, тому мета даної роботи – показати, що дана задача може бути розв'язана за субекспоненціальний час (швидкості росту такі, як $n^{\log n}$, які перевершують будь-який поліном, але менші ніж $2^{n^{\varepsilon}}$ для будь-якого ε >0, називають субекспоненціальними [8]).

Формалізація SAT задачі та її розв'язання

Розглянемо булеву функцію $f(x_1, x_2, .., x_n)$ в кон'юнктивній формі запису $f(x_1, x_2, .., x_n) =$

$$= (x_1^{\sigma_{11}} \vee x_2^{\sigma_{12}} \vee ... \vee x_n^{\sigma_{1n}}) \wedge ... \wedge (x_1^{\sigma_{m1}} \vee$$

$$\vee x_2^{\sigma_{m2}} \vee ... \vee x_n^{\sigma_{mn}}),$$

де $x_i^{\sigma} = \begin{cases} x_i, \text{ при } \sigma = 1 \\ \overline{x_i}, \text{ при } \sigma = 0 \end{cases}$.

Операції $\vee$, $\wedge$ є булеві і моделюють прості логічні висловлювання: $\vee$– «АБО»; $\wedge$– «ТА». Для будь-якого двійкового набору $x = (x_1, x_2, .., x_n)$ функція набуває одне з двох можливих значень: одиниця або нуль. Задача «выполнимость» полягає у відповіді на питання: чи існує набір значень змінних $\tilde{o} = (x_1, x_2, .., x_n)$, на яких функція f дорівнює одиниці.

Як показано в [9], SAT задачу можна розглядати як задачу про покриття, для цього по булевій функції побудуємо булеву матрицю *B*, в якій стовпцям відповідають змінні $(X_1, X_2, ..., X_n)$ і $(\overline{X}_1, \overline{X}_2, ..., \overline{X}_n)$, а рядкам - диз'юнкт булевої функції. У загальному випадку число стовпців в матриці *B* дорівнює *2n*, а число рядків дорівнює числу диз'юнктів *m* в булевій функції.

Наприклад, для булевої функції

$$F = (X_1 \vee X_2 \vee X_3)(\overline{X}_1 \vee \overline{X}_2 \vee \overline{X}_3) \cdot (X_1 \vee \overline{X}_3)(X_3 \vee \overline{X}_1)(X_1 \vee \overline{X}_2).$$

Перенумеруємо диз'юнкти булевої функції (табл. 1).

Таблиця 1

Нумерація диз'юнктів

1-$(X_1 \vee X_2 \vee X_3)$	2-$(\overline{X}_1 \vee \overline{X}_2 \vee \overline{X}_3)$	
3-$(X_1 \vee \overline{X}_3)$	4-$(X_3 \vee \overline{X}_1)$	5-$(X_1 \vee \overline{X}_2)$,

Тоді матриця *B* матиме вигляд

$$B = \begin{array}{c|cccccc} & X_1 & X_2 & X_3 & \overline{X}_1 & \overline{X}_2 & \overline{X}_3 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 & 1 & 1 \\ 3 & 1 & 0 & 0 & 0 & 0 & 1 \\ 4 & 0 & 0 & 1 & 1 & 0 & 0 \\ 5 & 1 & 0 & 0 & 0 & 1 & 0 \end{array}.$$

Стовпці, відповідні змінним X_i та $\overline{X}_i$ в матриці B, будемо називати інверсними. Якщо в матриці B існує покриття рядків одиницями, яке належить неінверсним стовпцям, то це означає, що функція f здійсненна, якщо такого покриття немає, то вона нездійсненна. Кожну змінну в матриці B, у загальному випадку з m рядками, тобто відповідної булевої функції з m диз'юнктів, будемо характеризувати вектором $H^{(i)}(h_1, h_2,\ldots, h_m)$, де $h_i = i$, якщо змінна X_i^{σ} покриває i-й рядок в матриці B і h_i =0, в протилежному випадку. У свою чергу кожному вектору припишемо вагову характеристику p_i, рівну числу компонент h_i, не рівних нулю. Якщо ми будемо розглядати підмножину з двох змінних X_i^{σ} і X_j^{σ} чи більш того, таку підмножину будемо характеризувати об'єднаним вектором $H^{(i,j\ldots)}$, в якому об'єднуються однойменні компоненти за правилом

$$i \bigcup i = i;\quad i \bigcup 0 = i,\ 0 \bigcup i = i;\quad 0 \bigcup 0 = 0. \qquad (1)$$

Наприклад, нехай задана булева функція

$$f = (x_2 \vee \overline{x_1} \vee \overline{x_3})\,(x_4 \vee \overline{x_2} \vee \overline{x_3})\,(x_2 \vee x_3 \vee \overline{x_4})\,(x_2 \vee \overline{x_1} \vee \overline{x_4})\,(x_1 \vee x_4 \vee \overline{x_2})\,(x_1 \vee x_2 \vee x_3) *$$
$$*\,(x_1 \vee x_3 \vee \overline{x_4})\,(x_1 \vee \overline{x_2} \vee \overline{x_3})\,(\overline{x_1} \vee \overline{x_2} \vee \overline{x_3})\,(x_2 \vee x_3 \vee \overline{x_1})\,(x_3 \vee \overline{x_2} \vee \overline{x_4})\,(x_1 \vee \overline{x_3} \vee \overline{x_4}). \qquad (2)$$

Перенумеруємо диз'юнкти

$$1\text{-}(x_2 \vee \overline{x_1} \vee \overline{x_3});\ 2\text{-}(x_4 \vee \overline{x_2} \vee \overline{x_3});\ 3\text{-}(x_2 \vee x_3 \vee \overline{x_4});$$
$$4\text{-}(x_2 \vee \overline{x_1} \vee \overline{x_4});\ 5\text{-}(x_1 \vee x_4 \vee \overline{x_2});\ 6\text{-}(x_1 \vee x_2 \vee x_3);$$
$$7\text{-}(x_1 \vee x_3 \vee \overline{x_4});\ 8\text{-}(x_1 \vee \overline{x_2} \vee \overline{x_3});\ 9\text{-}(\overline{x_1} \vee \overline{x_2} \vee \overline{x_3});$$
$$10\text{-}(x_2 \vee x_3 \vee \overline{x_1});\ 11\text{-}(x_3 \vee \overline{x_2} \vee \overline{x_4});\ 12\text{-}(x_1 \vee \overline{x_3} \vee \overline{x_4}).$$

Запишемо їх вектори $H^{(i)}$ з ваговими характеристиками, визначеними на основі введених правил (табл. 2).

Таблиця 2

Вектори $H^{(i)}$ з ваговими характеристиками

1	x_1	H^1(0,0,0,0,5,6,7,8,0,0,0,12)	p_1=4
2	x_2	H^2(1,0,3,4,0,6,0,0,0,10,0,0,0)	p_2 =5
3	x_3	H^3(0,0,3,0,5,6,7,0,0,1,0,0,0)	p_3 =5
4	x_4	H^4(0,2,0,0,5,0,0,0,0,0,0,0,0)	p_4 =2
5	$\overline{x_1}$	$H^{\bar{1}}$(0,0,0,4,0,0,0,0,9,10,0,0)	$p_{\bar{1}}$ =3
6	$\overline{x_2}$	$H^{\bar{2}}$(0,2,0,0,5,0,0,8,9,0,11,0)	$p_{\bar{2}}$ =5
7	$\overline{x_3}$	$H^{\bar{3}}$ (0,2,0,0,0,0,0,8,9,0,0,12)	$p_{\bar{3}}$ =4
8	$\overline{x_4}$	$H^{\bar{4}}$(0,0,3,4,0,0,7,0,0,0,11,12)	$p_{\bar{4}}$ =5

Всі пари X_i і $\overline{X}_i$, всі можливі множини, що не перетинаються та не містять інверсних вершин, на основі даних пар з їх об'єднаними векторами і їх ваговими характеристиками, визначеними відповідно до співвідношення (1), наведені в табл. 3, де вектори записані в дужках, а вагові характеристики векторів виділені більш жирним шрифтом.

З табл. 3 видно, що є підмножина $x_1\overline{x_3}\ x_2\overline{x_4}$ (1,2,3,4,5,6,7,8,9,10,11,12) p=**12=**m, що утворює покриття, і воно є виконуючим набором для вихідної булевої функції, в табл. 3 воно позначено зірочкою. Отже, якщо ми маємо довільну множину неінверсних змінних $\{X_i^{\sigma}\}$, для яких буде вагова характеристика $p_{i,\ldots,k} = m$ об'єднаного вектора $H^{(i,\ldots,k)}$, то це означає, що множина містить в собі підмножину, яка забезпечує здійсненність булевої функції, оскільки вона покриває всі рядки одиницями в матриці B. Розглянемо можливості побудови максимальних множин неінверсних змінних $\{X_i^{\sigma}\}$ для довільної булевої функції з n змінними. Розіб'ємо множину змінних булевої функції на два типи максимальних підмножин змінних, що не містять інверсних вершин. До перших віднесемо підмножини, які можна відразу кваліфікувати як максимальні, це підмножини

$$\{(x_1x_2x_3\ldots x_n);\ (\overline{x_1}\,\overline{x_2}\,\overline{x_3}\ldots\overline{x_n})\};$$
$$\{(x_1\overline{x_2}\,\overline{x_3}\ldots\overline{x_n});\ (x_2\overline{x_1}\,\overline{x_3}\ldots\overline{x_n})\ldots(x_n\overline{x_1}\,\overline{x_2}\ldots\overline{x_{n-1}})\}; \qquad (3)$$
$$\{(\overline{x_1}x_2x_3\ldots x_n);\ (\overline{x_2}x_1x_3\ldots x_n);\ldots..(\overline{x_n}x_1x_2\ldots x_{n-1})\},$$

їх всього $2n$ + 2. До другого типу віднесемо всі максимальні підмножини, які можна побудувати на основі об'єднання різними способами пар змінних X_i

і $\overline{X}_i$. Їх можна подати у вигляді дводольного графа, в якому ребрами пов'язані неінверсні змінні (рис. 1), при цьому кожна пара характеризується своїм вектором і ваговою характеристикою. Для функції з чотирма змінними всі такі пари наведені в першому стовпці табл. 3.

Таблиця 3

Етапи роботи процедури А

Всі можливі пари X_i та $\overline{X}_i$ і їх характеристики	Всі можливі об'єднання всіх неінверсних пар X_i та $\overline{X}_i$ і їх характеристики	Число підмножин з непарним числом змінних, які не будувалися процедурою А
1	**2**	**3**
$x_1\overline{x_2}$ (0,2,0,0,0,6,7,8,9,0,0,12) **7**	$x_1\overline{x_2}\ x_3\overline{x_4}$ (1,2,0,4,5,6,0,8,9,10,0,0) **8** $x_1\overline{x_2}\ x_4\overline{x_3}$ (0,2,3,4,5,6,7,8,0,0,0,0) **8**	$C_4^3 = 4$ $C_4^3 = 4$
$x_1\overline{x_3}$ (0,2,0,0,0,6,7,8,9,0,0,12) **6**	$x_1\overline{x_3}\ x_2\overline{x_4}$ (1,2,3,4,5,6,7,8,9,10,11,12) **12*** $x_1\overline{x_3}\ x_4\overline{x_2}$ (1,2,0,0,5,6,7,8,9,0,11,12) **9**	$C_4^3 = 4$ $C_4^3 = 4$
$x_1\overline{x_4}$ (0,0,3,4,0,6,7,8,0,0,11,12) **6**	$x_1\overline{x_4}\ x_2\overline{x_3}$ (1,2,3,4,5,6,7,8,9,0,11,12) **11** $x_1\overline{x_4}\ x_3\overline{x_2}$ (0,2,3,4,5,6,7,8,9,10,11,12)**11**	$C_4^3 = 4$ $C_4^3 = 4$
$x_2\overline{x_1}$ (1,0,3,4,0,6,0,0,9,10,0,12) **7**	$x_2\overline{x_1}\ x_4\overline{x_3}$ (1,2,3,4,5,6,7,8,9,0,11,12) **11** $x_2\overline{x_1}\ x_3\overline{x_4}$ (1,2,3,4,5,6,7,0,9,10,11,12)**11**	$C_4^3 = 4$ $C_4^3 = 4$
$x_2\overline{x_3}$ (1,2,0,0,0,6,7,8,9,0,0,12) **7**	$x_2\overline{x_3}\ x_1\overline{x_4}$ (1,2,3,4,0,6,7,8,9,0, 11,12) **10** $x_2\overline{x_3}\ x_4\overline{x_1}$ (1,2,0,4,5,6,7,8,9,10,0,12) **10**	$C_4^3 = 4$ $C_4^3 = 4$
$x_2\overline{x_4}$ (1,0,3,4,0,6,7,8,0,0,11,12)**7**	$x_2\overline{x_4}\ x_3\overline{x_1}$ (1,0,3,4,5,6,7,8,9,10,11,12)**11** $x_2\overline{x_4}\ x_1\overline{x_3}$ (1,2,3,4,0,6,7,8,9,0,11,12) **10**	$C_4^3 = 4$ $C_4^3 = 4$
$x_3\overline{x_1}$ (1,3,4,5,6,7,9,10,11) **9**	$x_3\overline{x_1}\ x_2\overline{x_4}$ (1, 2,3,4,5,6,7, 8,9,10,11,0) **11** $x_3\overline{x_1}\ x_4\overline{x_2}$ (1,2,3,4,5,6,7,8,9,10,11,0) **11**	$C_4^3 = 4$ $C_4^3 = 4$
$x_3\overline{x_2}$ (0,2,3,0,5,6,7,8,9,10,11,0)**9**	$x_3\overline{x_2}\ x_4\overline{x_1}$ (1,2,3,4,5,6,7,8,9,10,11,0) **11** $x_3\overline{x_2}\ x_1\overline{x_4}$ (0,2,3,4,5,6,7,8,9,10,11,12)**11**	$C_4^3 = 4$ $C_4^3 = 4$
$x_3\overline{x_4}$ (0,0,3,4,5,6,7,0,0,10,11,12) **8**	$x_3\overline{x_4}\ x_1\overline{x_2}$ (0,2,3,4,5,6,7,8,9,10,11,12)**11** $x_3\overline{x_4}\ x_2\overline{x_1}$ (1,0,3,4,5,6,7,9,10,11,12) **11**	$C_4^3 = 4$ $C_4^3 = 4$
$x_4\overline{x_1}$ (1,2,0,4,5,0,0,0,9,10,0,0) **6**	$x_4\overline{x_1}\ x_2\overline{x_3}$ (1,2,0,4,5, 6,7,8,9,10,12) **11** $x_4\overline{x_1}\ x_3\overline{x_2}$ (1,2,3,4,5,6,7,8,9,10,11,0) **11**	$C_4^3 = 4$ $C_4^3 = 4$
$x_4\overline{x_2}$ (0,2,0,0,5,0,0,8,9,0,11,0) **5**	$x_4\overline{x_2}\ x_1\overline{x_3}$ (0,2,0,0,5, 6,7,8,9,0,11,12) **8** $x_4\overline{x_2}\ x_3\overline{x_1}$ (1,2,3,4,5,6,7,8,9,10,11,0) **11**	$C_4^3 = 4$ $C_4^3 = 4$
$x_4\overline{x_3}$ (1,2,0,0,5,0,0,8,9,0,0,12) **6**	$x_4\overline{x_3}\ x_1\overline{x_2}$ (1,2,0,0,5,6,7,8,9,0,0,12) **8** $x_2\overline{x_1}$ (1,2,3,4,5,6,0,8,9,10,0,12) **10**	$C_4^3 = 4$ $C_4^3 = 4$ Всього неявно побудовано 2^7=128 підмножин з непарним числом змінних

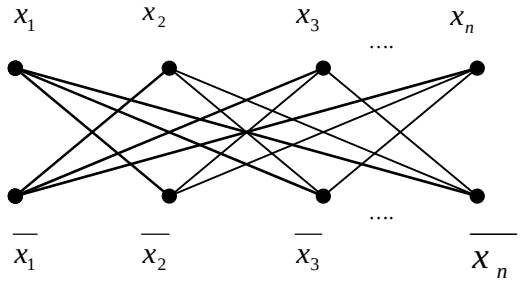

Рис. 1. Граф, що відображає пари неінверсних змінних

Розглянемо процедуру А формування максимальних множин, що не містять інверсних вершин.

Процедура А

Крок 1. Формуємо всі множини змінних булевої функції першого типу, їх вектори $H^{(i)}(h_1, h_2,\ldots, h_m)$ і визначаємо їх вагові характеристики p_i.

Крок 2. Перевіряємо, чи є множини з $p_i=m$, якщо немає, то виконуємо наступний крок, інакше процедура закінчує роботу, оскільки аналізована булева функція здійсненна.

Крок 3. З пар X_i та $\overline{X}_i$ формуємо всі можливі множини, що містять подвійну кількість змінних та не містять інверсних вершин, і перевіряємо, чи є серед отриманих множин множини з ваговою характеристикою $p_i =m$, якщо так, то булева функція здійсненна і процедура закінчує роботу, якщо ні, то виконуємо наступний крок.

Крок 4. З усіх поточних множин об'єднуємо ті, що не перетинаються за елементами підмножини і не містять інверсних вершин, і знову отримуємо підмножини з подвоєною кількістю змінних, що не містять інверсних вершин. Перевіряємо, чи є серед отриманих множин множини з ваговою характеристикою $p_i =m$, якщо так, то булева функція здійсненна і процедура закінчує роботу, якщо ні, то виконуємо наступний крок.

Крок 5. Перевіряємо, чи досягла потужність сформованих множин величини n, якщо n парне, або $(n\text{-}1)$, якщо n непарне, якщо ні, то переходимо до виконання кроку 4, інакше виконуємо наступний крок.

Крок 6. Перевіряємо, чи є серед отриманих множин множини з ваговою характеристикою $p_i =m$, якщо так, то булева функція здійсненна, якщо ні, то булева функція нездійсненна.

Фактично, в процедурі ***А*** процес подвоєння множин продовжує повторюватися до тих пір, поки на основі отриманих підмножин подальше об'єднання стає неможливим через наявність інверсних вершин або подальше об'єднання не змінює отриманих підмножин. Зрозуміло, що така ситуація настане на кроці k роботи процедури ***А***, коли потужність сформованих підмножин досягне величини (n), якщо n парне, або $(n\text{-}1)$, якщо n непарне. Особливістю роботи процедури є те, що максимальні множини, що не містять непарного числа змінних, завжди будуть міститися як підмножини в підмножинах з парним числом змінних, але на одиницю більших. Число підмножин, що не явно будувалися процедурою А, за кожним об'єднанням наведеним в стовпці 2 табл. 3 записані в третьому стовпці табл. 3.

Число підмножин, сформованих на першому кроці роботи процедури, дорівнюватиме $n(n\text{-}1)$, на другому $n(n\text{-}1)$ $(n\text{-}2)$ і т.д. на наступних кроках буде підсумовуватися, що відбивається співвідношенням (4)

$$n(n\text{-}1)+n(n\text{-}1)(n\text{-}2)+ n(n\text{-}1)(n\text{-}2)(n\text{-}4)+ n(n\text{-}1)(n\text{-}2)(n\text{-}4)(n\text{-}8)\ldots +\ldots . \quad (4)$$

Перепишемо (4) в такому вигляді:

$$n(n\text{-}1)[1+(n\text{-}2^1)+ (n\text{-}2^1)\ (n\text{-}2^2)+\ldots.+ (n\text{-}2^1)\ (n\text{-}2^2)\ (n\text{-}2^3)\ldots\ (n\text{-}2^k)] = n(n\text{-}1)b. \quad (5)$$

Процес підсумовування в (5) повинен припинитися на k-му кроці, після досягнення значення $2^k = n$, тобто при $k = log_2(n)$, коли в останньому доданку число співмножників стане рівне $log_2\ (n)$. Як видно з (5), справедлива нерівність

$$b < n^0+n^1+ n^2+ n^3+\ldots + n^{\log_2 n} . \quad (6)$$

Вважаючи в (6) всі $n^i = n^{\log_2 n}$, можна записати нерівність (7)

$$n^0+n^1+ n^2+ n^3+\ldots + n^{\log_2 n} < \log_2(n) n^{\log_2 n+1} . \quad (7)$$

З (5) і (7) випливає, що число множин, які доведеться побудувати процедурі А, не перевищить $\log_2(n) n^{\log_2 n+3}$, а число операцій для формування цих множин не перевищить $m \log_2(n) n^{\log_2(n)+4}$. З урахуванням формування множин першого типу сумарна складність побудови максимальних множин, що не містять інверсних вершин, буде дорівнювати

$$\boldsymbol{O}(m\log_2(n)n^{\log_2(n)+4} + mn(2n+2)) \approx \boldsymbol{O}. \quad (8)$$

Роботу процедури А для прикладу (2) можна простежити за допомогою табл. 3, в якій в першому стовпці розташовані всі пари неінверсних змінних за винятком пар, що відповідають типу 1. Процес формування множин, що містять по чотири змінних, можна відобразити у вигляді графа (рис. 2).

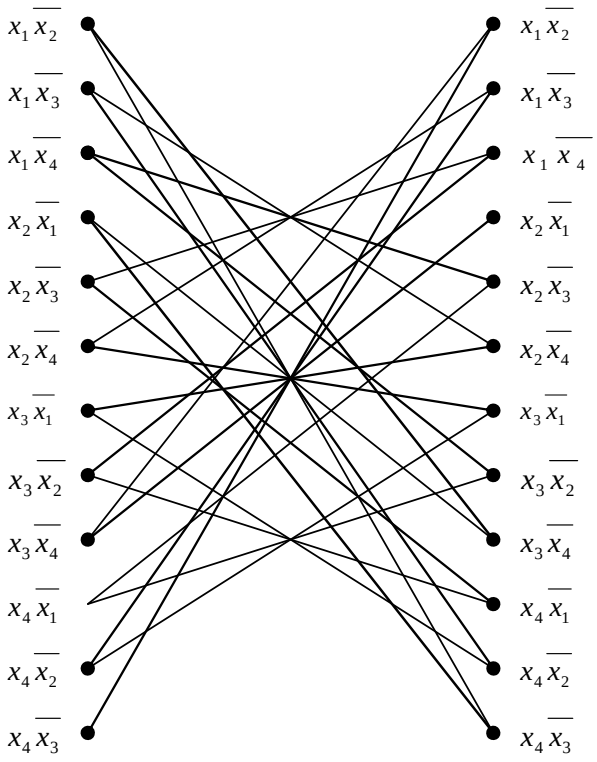

Рис. 2. Граф *G* для пошуку максимальних множин, що не містять інверсних вершин

У графі *G* на рис. 2 вершинам відповідають пари неінверсних змінних і підмножини вершини з'єднані ребрами, якщо підмножини не перетинаються і не містять інверсних змінних. У загальному випадку ступені вершин в графі *G*, наведеному на рис. 2, рівні *n*-2, а для розглянутого прикладу 4-2=2. Результати об'єднання підмножин наведені в другому стовпці табл. 3. У третьому стовпці табл. 3 наведена кількість об'єднань змінних по три, які процедура не явно побудувала, їх загальна кількість дорівнює 2^7=128. Оскільки число елементів в підмножинах дорівнює n, подальше об'єднання не має сенсу, так як множини або будуть перетинатися, або не будуть змінюватися. Як випливає з табл. 3, у нас для прикладу (2) виконуючою є тільки одна множина змінних $x_1\overline{x_3}\ x_2\overline{x_4}$ (1,2,3,4,5,6,7,8,9,10,11,12) з вагою *p*=**12=*m*,** оскільки легко перевірити, що жодна підмножина першого типу не дає ваги *p*=**12=*m***. Слід зазначити, що якщо граф G побудований для деякої довільної булевої функції з n змінними, то початковий ступінь вершин буде n-2, при наступних об'єднаннях, по 2, по 4, по 8 і т.д., ступені вершин в графах, в яких ці підмножини відповідатимуть вершинам графа, будуть зменшуватися по експоненті і при цьому множини з непарним числом змінних перераховуються автоматично і на них процедура спеціально не витрачає часу, так як вони містяться в тих, які процедура А перераховує. Це видно зі співвідношення (5), чим і пояснюється той факт, що число максимальних множин складалося з інверсних змінних і що процедура А перераховує ці максимальні множини з НЕінверсних змінних за субекспоненціальний час.

Висновок

Таким чином, для SAT задачі запропоновано алгоритм субекспоненціальної складності при $\varepsilon = 1$. Зрозуміло, що складність процедури А досить висока, але якщо взяти відношення $\frac{2^n}{n^{\log_2 n}}$, наприклад при n=100 і n=1000, то отримаємо відповідно $1{,}3\cdot10^{16}$ і $1{,}1\cdot10^{271}$, тобто часовий виграш потенційно може бути суттєвим. Слід зазначити, що процедура А в разі нездійсненних функцій перераховує всі максимальні набори неінверсних змінних і робить в гіршому випадку число кроків, що визначається співвідношенням (8), тобто з її допомогою можна перерахувати за субекспоненціальний час всі набори змінних, на яких булева функція набуває значення «істинно», при цьому процедура А набуває такого вигляду:

Процедура А/

Крок 1. Формуємо всі підмножини змінних булевої функції першого типу, їх вектори $H^{(i)}(h_1, h_2,\ldots, h_m)$ і визначаємо їх вагові характеристики p_i.

Крок 2. Перевіряємо, чи є множини з p_i=*m*, якщо ні, то виконуємо наступний крок, інакше запам'ятовуємо даний набір змінних і заносимо його в множину В, оскільки аналізована булева функція на даному наборі здійсненна.

Крок 3. З пар X_i і $\overline{X}_i$ формуємо всі можливі множини, що містять подвійну кількість змінних та не містять інверсних вершин. Далі перевіряємо серед отриманих множин, чи є множини з ваговою характеристикою p_i =*m*, якщо так, то булева функція здійсненна на відповідних наборах, ми їх заносимо в множину В, якщо ні, то виконуємо наступний крок.

Крок 4. З усіх поточних множин об'єднуємо тільки ті, що не перетинаються за елементами підмножини і не містять інверсних вершин, і знову отримуємо

підмножини з подвоєною кількістю змінних, що не містять інверсних вершин. Перевіряємо, чи є серед отриманих множин множини з ваговою характеристикою $p_i = m$, якщо так, то булева функція здійсненна на відповідних наборах, ми їх заносимо в множину В, якщо ні, то виконуємо наступний крок.

Крок 5. Перевіряємо, чи досягла потужність сформованих множин величини n, якщо n парне, або (n-1), якщо n непарне, якщо ні, то переходимо до виконання кроку 4, інакше виконуємо наступний крок.

Крок 6. Перевіряємо в множині В, чи є множини з ваговою характеристикою $p_i = m$, якщо так, то булева функція здійсненна і всі множини в В визначають набори, на яких функція здійсненна, якщо ні, то булева функція нездійсненна.

Наведена процедура A' дозволяє перерахувати всі набори змінних, на яких булева функція, що аналізується, здійсненна за субекспоненціальний час, тобто розв'язати задачу «полная выполнимость». Зазначений результат буде слугувати базою покращення інформаційно-вимірювальних компонентів та інформаційно-керуючих систем залізничного транспорту.

Список використаних джерел

1. Бутенко, В. М. Компьютерная система управления движением поездов [Текст] / В. М. Бутенко, В. И. Мойсеєнко, Д. М. Кузьменко // Залізничний транспорт України. – 2000. – № 5–6. – С. 80–82.
2. Комутаційний пристрій-оптоелектронний аналог електромагнітного реле струму [Текст] : пат. UA № 116449, МПК[9] H03K 17/60 (2006.01) / Бутенко В. М., Головко О. В., Зайченко О. Б., Мелешко В. В., Мірошник М. А., Мойсеєнко В. І., Чуб І. М., Чуб С. Г.; заявник і власник Український державний університет залізничного транспорту. – № u 2016 11255 від 07.11.2016; опубл. 25.05.2017, Бюл. № 10. – 8 с.
3. Пристрій підвищення точності обліку і контролю електроенергії вимірювальним комплексом [Текст] : пат. UA № 102949, МПК[9] H 01F 38/00; H 01F 38/20; H 01F 38/28; G01R 21/00; G01R 21/06; G01R 22/00 / Бутенко В. М., Білоусов О. Ф., Бриксін В. О., Головко О. В., Махота А. О., Приходько Ю. С., Терьошин В. М.; Скарговській А. О., Терьошин О. В.; заявник і власник Українська державна академія залізничного транспорту. - № a 2012 08136 від 03.07.2012; опубл. 27.08.2013, Бюл. № 16. – 6 с.
4. Математичне моделювання в розподілених інформаційно-керуючих системах залізничного транспорту [Текст] : монографія / С. В. Лістровий, С. В. Панченко, В. І. Мойсеєнко, В. М. Бутенко – Харків : ФОП Бровін О.В., 2017. – 220 с.
5. Development of method of definition maximum clique in a non-oriented graph [Text] / S. V. Listrovoy, V. M. Butenko, V. O. Bryksin, O. V. Golovko // EasternEuropean Journal of Enterprise Technologies. – 2017. – Vol. 5, №4 (89). – P. 12 – 17. DOI: 10.15587/1729-4061.2017.111056
6. Signal flow graph models and alternative gain formula for multiprobe microwave multimeter [Text] / Zaichenko O.B., Butenko V.M., Miroshnyk M.A. // Інформаційно-керуючі системи на залізничному транспорті. – 2016. – №12 (98). – С. 12–17.
7. Бутенко, В. М. Оптимізація моделей розподілених інформаційно-вимірювальних систем залізничного транспорту [Текст] / В. М. Бутенко // Прикладні науково-технічні дослідження: матеріали Міжнар. наук.-практ. конф. (5-7 квітня 2017). – Івано-Франківськ : «Симфонія форте», 2017. – С. 88–89.
8. Скатов, А. В. Аппаратное ускорение решения задач выполнимости для построения тестов цифровых схем [Текст] / А. В. Скатов, А. В. Борисевич // Информатика, электроника, связь: сб. науч. тр. – Севастополь : Изд-во Сев. НТУ, 2008. – С. 9–15.
9. Kheterpal V., Rovner V. V., Hersan T. G., Motiani D., Takegawa Y., Strojwas A. J., and Pileggi L. Design Methodology for IC Manufacturability Based on Regular Logic Bricks. In Proceedings of the 42nd Conference on Design Automation, pages 353–358, 2005.
10. Taylor B., Pileggi L. Exact Combinatorial Optimization Methods for Physical Design of Regular Logic Bricks. In Proceedings of the 44th Conference on Design Automation, P. 344–349, 2007.
11. Cheremisinova L., Novikov D. SAT-Based Approach to Verification of Logical Descriptions with Functional Indeterminacy // 8th International Workshop on Boolean Problems. Freiberg: September 18 – 19, 2008. – P. 59–66.
12. Дулькейт, В. И. Непрерывные аппроксимации решения задачи «выполнимость» применительно к криптографическому анализу асиммет-ричных шифров [Текст] / В. И. Дулькейт, Р. Т. Файзуллин , И. Г. Хныкин // Компьютерная оптика. – 2009. – №1, Т. 33. – С. 86–90.
13. Listrovoy, S.V. On Correlation of P And NP Classes [Text] / S.V. Listrovoy // I. J. Modern Education and Computer Science. – 2012. – № 3. – P. 21–27.
14. Спосіб вимірювання параметрів сигналів і трактів НВЧ [Текст] : пат. UA № 113161, Україна, МПК G01R 21/04; G01R 27/06 / Зайченко О. Б., Ключник І. І., Мірошник М. А., Бутенко В. М.; заявник і патентовласник Харківський національний ун-т радіоелектроніки; заявл. – № u 2016 08483 від 01.08.2016; опубл. 10.01.2017, Бюл. № 1. – 5 с.

Бойник А. Б., Бутенко В. М., Головко А. В., Ушаков М. В. Оптимизация алгоритма субэкспоненциальной сложности для решения SAT задачи. При модернизации и создании современных систем управления на железнодорожном транспорте создаются оптоэлектронные аналоги электромагнитных реле. При их построении возникает необходимость решения в реальном времени задачи выполнимости булевых формул (SAT задача). В данной работе для SAT задачи предложен алгоритм субэкспоненциальной сложности, который определяет, осуществима ли функция, а также процедура, которая позволяет перечислить все наборы переменных, на которых булева функция осуществима за субэкспоненциальное время.
Ключевые слова: SAT задача, булева функция, субэкспоненциальная сложность.

Boinik A. B., Butenko V. M., Golovko O. V., Ushakov M. V. Optimization of subexponential complexity algorithm for SAT problem solution. During the modernization and creation of modern control systems on railway transport, new modern optoelectronic analogues of electromagnetic relays are being created. When constructing them, it becomes necessary to model the interaction of nodes. To this end, Boolean functions of algebra-logic are constructed, which can be of a high degree of complexity and contain a large number of clauses. Further, there arises the need to solve the Boolean satisfiability problem in real time (SAT task), and in the case of the feasibility of the task it is additionally necessary to specify all the sets of variables for which it is true. The algorithms described in the literature at the present time have an exponential dependence of complexity on the number of changes and complexity of the function, and accordingly the execution time increases exponentially with the complexity of the function. In this paper, a subexponential complexity algorithm for the SAT task, which determines whether a function is feasible is proposed, and also a procedure that allows you to enumerate all sets of variables under which the Boolean function being analyzed can be realized for subexponential time. This makes it possible to achieve a significant gain in time with Boolean functions with a large number of changes and clauses.
Keywords: SAT task, boolean function, subexponential complication.

Бойнік Анатолій Борисович, *доктор технічних наук, професор кафедри "Автоматика та комп'ютерне телекерування рухом поїздів", Український державний університет залізничного транспорту, Харків, Україна. E-mail: boynik.ab@kart.edu.ua http://orcid.org/0000-0001-7773-9055*

Бутенко Володимир Михайлович*, кандидат технічних наук, доцент кафедри «Спеціалізовані комп'ютерні системи», Український державний університет залізничного транспорту, пл. Фейєрбаха, 7, м. Харків, Україна, 61050 E-mail: butenko@kart.edu.ua , http://orcid.org/0000-0001-9958-3960*

Головко Олександра Володимирівна*, кандидат технічних наук, доцент кафедри «Обчислювальної техніки та систем управління», Український державний університет залізничного транспорту, пл. Фейєрбаха, 7, м. Харків, Україна, 61050, E-mail: golovko@kart.edu.ua, http:// orcid.org/0000-0002-9880-428X*

Ушаков Михайло Віталійович*, старший викладач кафедри "Автоматика та комп'ютерне телекерування рухом поїздів", Український державний університет залізничного транспорту, Харків, Україна. E-mail: micush@kart.edu.ua http://orcid.org/0000-0001-6270-4212*

Anatolii Boinik*, Doctor of engineering, Professor at the Department of "Automation and computer control of the movement of trains", Ukrainian State University of Railway Transport, Kharkiv, Ukraine. E-mail: boynik.ab@kart.edu.ua . http://orcid.org/0000-0001-7773-9055*

Butenko Volodymyr M., *PhD, Associate Professor department of specialized computer systems, Ukrainian State University of Railway Transport, Kharkiv, Ukraine. E-mail: butenko@kart.edu.ua ORCID: http:// orcid.org/0000-0001-9958-3960*

Golovko Oleksandra V., *PhD, Associate Professor department of Computer Engineering and Control Systems, Ukrainian State University of Railway Transport, Kharkiv, Ukraine. E-mail: golovko@kart.edu.ua http:// orcid.org/0000-0002-9880-428X*

Mykhailo Ushakov*, Senior Lecturer at the Department of "Automation and computer control of the movement of trains", Ukrainian State University of Railway Transport, Ukrainian State University of Railway Transport, Kharkiv, Ukraine. E-mail: micush@kart.edu.ua http://orcid.org/0000-0001-6270-4212*

Надійшла 23.04.2018 р.