КІБЕРНЕТИКА

УДК 519.713.4

І.К. РИСЦОВ
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна,
e-mail: *haryst49@gmail.com*.

ПРОБЛЕМА ЧЕРНІ ДЛЯ АВТОМАТІВ ІЗ ПРОСТИМИ ІДЕМПОТЕНТАМИ

Анотація. Отримано дві точні оцінки функції Черні $C(A)$ для автоматів із простими ідемпотентами (ПІ-автоматів). Показано, що $C(A) = n-1$ для ПІ-автомата A з n станами і тривіальною групою та $C(A) \le (n-1)^2$ для ПІ-автомата A з n станами і регулярною групою.

Ключові слова: скінченні автомати, проблема Черні.

У праці [1] в 1964 р. Я. Черні висловив гіпотезу про те, що у будь-якому синхронізованому скінченному автоматі із n станами існує зворотне слово довжиною $(n-1)^2$, яке переводить усі стани автомата в єдиний стан. За минулий час гіпотезу Черні вдалося довести для окремих класів автоматів [2–5], проте в загальному випадку вона поки що залишається відкритою.

У цій роботі гіпотезу Черні буде доведено для одного класу автоматів із простими ідемпотентами. Цей результат випливає з робіт [6, 7], тому цю статтю можна розглядати як їхнє продовження і завершення.

СКІНЧЕННІ АВТОМАТИ

Нехай S — скінченна множина, що складається з n елементів $|S| = n$, тоді позначимо $\mathrm{End}(S)$ множину всіх перетворень (морфізмів) на цій множині $\mathrm{End}(S) = \{f \mid f : S \to S\}$. Число $|\mathrm{im}(S)|$ називається рангом морфізма f, а число $\mathrm{df}(f) = |S| - |\mathrm{im}(S)|$ — його дефектом.

Нагадаємо, що моноїдом M називається множина з асоціативною бінарною операцією і одиницею. Множина $\mathrm{End}(S)$ є моноїдом щодо операції композиції морфізмів (функцій) і називається повним моноїдом морфізмів на множині S. Моноїдом морфізмів називається підмоноїд повного моноїда.

Позначимо $\mathrm{End}_k(S)$ підмножину морфізмів, ранг яких становить не більше ніж k, $1 \le k \le n$. Ці підмножини утворюють зростальний ланцюг ідеалів $\mathrm{End}_1(S) \subset \mathrm{End}_2(S) \subset \ldots \subset \mathrm{End}_n(S) = \mathrm{End}(S)$ повного моноїда морфізмів. Морфізми з мінімального ідеалу $\mathrm{End}_1(S)$ мають одиничний ранг і називаються константними морфізмами (константами), оскільки вони відображають всі елементи із S в один елемент.

Скінченним детермінованим автоматом (без виходу) називається трійка $A = (S, X, F)$, де S — скінченна множина станів, X — скінченний вхідний алфавіт, F — функція переходів, яка є відображенням вигляду $F: S \times X \to S$. Число $n = |S|$ називається числом станів автомата A.

Множина всіх слів X^* в алфавіті X називається вільним моноїдом, оскільки X^* є моноїдом щодо операції конкатенації слів. Функція переходів автомата індуктивно визначається на всіх словах $w \in X^*$ за формулою

$$F(s, x_1 \ldots x_{k-1} x_k) = F(F(s, x_1 \ldots x_{k-1}), x_k).$$

Довжина слова $w = x_1 \ldots x_k$ позначається $l(w) = k$. Надалі $F(s, w)$ буде означати стан, в який переходить автомат під дією слова w.

З розширеною функцією переходів $F: S \times X^* \to S$ можна пов'язати гомоморфізм моноїдів $F_A : X^* \to \mathrm{End}(S)$, якщо кожному слову $w \in X^*$ зіставити морфізм $F_A(w) = f_w$, який визначається за формулою

$$f_w(s) = F(s, w) \text{ для всіх } s \in S. \tag{1}$$

Гомоморфізм F_A називається канонічним гомоморфізмом автомата A, а його образ $M_A = F_A(X^*)$ — моноїдом переходів автомата A.

Вхідне слово w називається зворотним для автомата $A = (S, X, F)$, якщо морфізм $F_A(w)$ є константою, тобто $F_A(w) \in \mathrm{End}_1(S)$. З формули (1) випливає, що зворотне слово переводить всі стани автомата в один стан $F(S, w) = \{s\}$. Автомат A називається синхронізованим, якщо у нього є зворотне слово. Позначимо $C(A)$ довжину найкоротшого зворотного слова в синхронізованому автоматі A.

Автомат A називається транзитивним (або сильно зв'язним), якщо з кожного його стану можна досягти будь-якого стану. Надалі, якщо не визначено інше, вважатимемо, що розглядаються транзитивні автомати.

Образом підмножини станів $T \subseteq S$ під дією слова w називається підмножина $F(T, w) = \{F(s, w) : s \in T\}$. Прообраз підмножини $T \subseteq S$ під дією слова w визначається за формулою $F^{-1}(T, w) = \{s : F(s, w) \in T\}$. Слово w називається збільшувальним для підмножини T, якщо справджується нерівність $|F^{-1}(T, w)| > |T|$. Скінченний набір вхідних слів W називається збільшувальним для автомата A, якщо для будь-якої нетривіальної підмножини його станів T $(\varnothing \subset T \subset S)$ в наборі W існує слово, що збільшує підмножину T. Автомат A називається спрямованим, якщо у нього є збільшувальний набір слів. Твердження, що наведене далі, визначає критерій спрямованості автомата [6, 7].

Пропозиція 1. Автомат буде спрямованим тоді і тільки тоді, коли він синхронізований і транзитивний.

Довжиною $l(W)$ набору слів W вважатимемо максимальну довжину слів, які входять до нього. Позначимо $\mathrm{inc}(A)$ довжину найкоротшого набору збільшувальних слів у спрямованому автоматі A. Сформульоване далі твердження уточнює і посилює попередню пропозицію [6].

Пропозиція 2. Нехай A — спрямований автомат з n станами, тоді має місце нерівність $C(A) \le \mathrm{inc}(A) \cdot (n-2) + 1$.

Зокрема, якщо $\mathrm{inc}(A) \le n$, то $C(A) \le (n-1)^2$, тобто для таких автоматів справедлива гіпотеза Черні. Ця стратегія доказу гіпотези Черні отримала назву «зворотного методу», оскільки вона ґрунтується на збільшенні прообразів підмножини станів. Пізніше з'ясувалося, що ця стратегія не є універсальною, однак, як буде доведено, для автоматів із простими ідемпотентами вона «працює».

Морфізм $f: S \to S$ називається ідемпотентом, якщо $f \circ f = f$. Ця умова рівнозначна тому, що морфізм f діє тотожно на своїй області значень, тобто $f(s) = s$ для всіх $s \in \mathrm{im}(f)$. Ідемпотент f називається простим, якщо його дефект дорівнює одиниці, $\mathrm{df}(f) = 1$, або, що рівносильно, $\mathrm{im}(f) = |S| - 1$. У цьому разі є точно один стан $s \in S \setminus \mathrm{im}(f)$, який позначимо $h(f)$, що під дією f переходить у відмінний від нього стан $t(f)$, а інші стани залишаються нерухомими.

Отже, простий ідемпотент f визначає нетривіальну впорядковану пару станів $(h(f), t(f))$, де $h(f) \neq t(f)$, і, навпаки, кожна нетривіальна впорядкована пара станів (s, u) визначає простий ідемпотент f такий, що $(s, u) = (h(f), t(f))$. Значить, на множині S, що складається з n станів, у повному моноїді $\mathrm{End}(S)$ є точно $n^2 - n$ простих ідемпотентів.

Нехай $A = (S, X, F)$ — скінченний автомат, тоді кожен вхідний символ $x \in X$ визначає за формулою (1) базовий морфізм $F_A(x) = f_x$. Вхідний символ $x \in X$ назвемо простим ідемпотентом автомата A, якщо морфізм $f_x: S \to S$ є простим ідемпотентом. Покладемо для стислості $h(x) = h(f_x)$ і $t(x) = t(f_x)$, тоді для кожного простого ідемпотенту $x \in X$ в автоматі A виконуються такі умови:

$$F(h(x), x) = t(x), \ F(s, x) = s \text{ для всіх } s \neq h(x). \tag{2}$$

Вхідний символ $x \in X$ автомата $A = (S, X, F)$ назвемо груповим, якщо базовий морфізм $f_x: S \to S$ є бієкцією (переставленням) на множині станів. Зауважимо, що дефект будь-якої бієкції дорівнює нулю. Підмножина базових бієкцій $\{f_x: \mathrm{df}(f_x) = 0\}$ автомата A породжує групу переставлень $G(A) = \langle f_x: \mathrm{df}(f_x) = 0 \rangle$, яка називається групою автомата A. Автомат називається груповим, якщо всі його вхідні символи є груповими.

Означення 1. Негруповий автомат $A = (S, X, F)$ назвемо автоматом із простими ідемпотентами (ПІ-автоматом), якщо кожен його вхід $x \in X$ є або простим ідемпотентом, або груповим символом.

Отже, в ПІ-автоматі A для будь-якого $x \in X$ справджуються нерівності

$$0 \leq \mathrm{df}(f_x) \leq 1. \tag{3}$$

Тому відповідно до нерівностей (3) множина входів X ПІ-автомата A розбивається на дві частини: $X = I \cup Y$, в першу з яких потрапляють прості ідемпотенти $I = \{x: \mathrm{df}(f_x) = 1\}$, а в другу — групові входи $Y = \{x: \mathrm{df}(f_x) = 0\}$. За означенням 1 підмножина I має бути непорожньою, а підмножина Y може бути порожньою. У цьому разі група $G(A)$ автомата A вважається тривіальною, що складається з тотожного морфізма 1_S (одиниця групи).

У ПІ-автоматі $A = (S, X, F)$ для будь-якого $x \in I$ і будь-якої підмножини $T \subseteq S$ виконується така умова:

$$F^{-1}(T, x) = \begin{cases} T \cup \{h(x)\}, & \text{якщо } t(x) \in T, \\ T \setminus \{h(x)\}, & \text{якщо } t(x) \notin T. \end{cases} \tag{4}$$

Дійсно, з формули (2) випливає, що $F(h(x), x) = F(t(x), x) = t(x)$, отже, $F^{-1}(T, x) = T \cup \{h(x)\}$, якщо $t(x) \in T$. Друга альтернатива випливає з умови $F^{-1}(h(x), x) = \varnothing$ і $F^{-1}(s, x) = s$ для всіх $s \in S \setminus \{h(x), t(x)\}$. Звідси отримуємо таке твердження.

Пропозиція 3. Простий ідемпотент $x \in I$ буде збільшувати підмножину станів T в ПІ-автоматі A тоді і тільки тоді, коли $h(x) \notin T$ і $t(x) \in T$.

Крім того, з властивості (4) випливає пропозиція, яку доведено в роботі [7].

Пропозиція 4. Нехай w — найкоротше слово, яке збільшує підмножину станів T в ПІ-автоматі A, тоді $w = xy_1 \ldots y_m$, де $x \in I$ і $y_i \in Y$, $1 \le i \le m$.

Звідси отримуємо такий результат.

Теорема 1. Нехай $A = (S, I, F)$ — синхронізований ПІ-автомат з n станами і тривіальною групою $G(A) = \{1_S\}$, тоді $C(A) = n - 1$.

Доведення. Зауважимо, що $C(A) \ge n - 1$, оскільки кожен простий ідемпотент склеює тільки два стани. Якщо A — сильно зв'язний автомат, то згідно з пропозицією 1 він буде спрямованим. Тоді згідно з пропозицією 4 маємо, що $\mathrm{inc}(A) = 1$, бо в автоматі A немає групових символів. Отже, будь-яка нетривіальна підмножина станів може бути збільшена одним ідемпотентом. Звідси і з пропозиції 2 випливає, що $C(A) \le n - 1$.

Однак вимога сильної зв'язності є у такому разі зайвою. Дійсно, оскільки автомат A синхронізований, у нього є стан s_0, який буде досяжним з усіх станів. Тоді, поклавши стан s_0 як корінь, побудуємо орієнтоване дерево досяжності T, дуги якого відповідають простим ідемпотентам $x_1, \ldots, x_{n-1}$. Кожен символ x_i знижує на одиницю висоту тільки однієї вершини s_i, $1 \le i \le n - 1$, а висоти інших вершин залишаються незмінними. Тому простий алгоритм, що знижує висоту максимальної за висотою вершини, дає зворотне слово довжини $n - 1$.

Теорему доведено.

ОРБІТАЛЬНІ ГРАФИ ГРУПИ ПЕРЕСТАВЛЕНЬ

Надалі знадобляться деякі поняття з теорії графів. Поставимо бінарному відношенню $\rho \subseteq S \times S$ у відповідність орієнтований граф (орграф) $\Gamma(\rho) = (S, \rho)$ з множиною вершин S і множиною дуг ρ, а також неорієнтований граф $\Gamma[\rho]$, який отримуємо з $\Gamma(\rho)$ заміною всіх дуг неорієнтованими ребрами.

Позначимо $\zeta(\rho)$ відношення досяжності в орграфі $\Gamma(\rho)$, тобто $(s, t) \in \zeta(\rho)$, якщо існує шлях в орграфі $\Gamma(\rho)$ зі стану s у стан t. Зауважимо, що $\zeta(\rho)$ буде транзитивним замиканням відношення ρ. Розглянемо відношення сильної зв'язності $\gamma(\rho) = \zeta(\rho) \cap \zeta(\rho)^{-1}$ і слабкої зв'язності $\varepsilon(\rho)$ в орграфі $\Gamma(\rho)$, де $\varepsilon(\rho)$ — еквівалентне замикання відношення ρ. Обидва ці відношення будуть відношеннями еквівалентності, а їхні класи називаються відповідно компонентами сильної і слабкої зв'язності орграфу $\Gamma(\rho)$. Зауважимо, що слабко зв'язні компоненти орграфу $\Gamma(\rho)$ збігаються з компонентами зв'язності неорієнтованого графу $\Gamma[\rho]$, тому між ними немає сполучних дуг орграфу $\Gamma(\rho)$. Відзначимо також, що $\gamma(\rho)$ буде найбільшою (за включенням) еквівалентністю, що міститься у відношенні $\zeta(\rho)$, а $\varepsilon(\rho)$ — найменшою еквівалентністю, що включає відношення $\zeta(\rho)$. Звідси отримуємо такі включення для будь-якого $\rho \subseteq S \times S$:

$$\gamma(\rho) \subseteq \zeta(\rho) \subseteq \varepsilon(\rho). \tag{5}$$

Орграф $\Gamma(\rho) = (S, \rho)$ називається сильно зв'язним, якщо з будь-якого його стану існує шлях у будь-який інший стан, тобто $\zeta(\rho) = S \times S$. Тоді на основі властивості (5) робимо висновок, що в цьому разі виконуються рівності

$$\gamma(\rho) = \zeta(\rho) = \varepsilon(\rho) = S \times S.$$

Тому сильно зв'язний орграф має тільки одну компоненту сильної (і слабкої) зв'язності, яка збігається з усією множиною S.

Вважатимемо, що пара (або дуга орграфу) (s, t) перетинає підмножину станів T, якщо $s \notin T$ і $t \in T$. Неважко довести такий критерій сильної зв'язності [8].

Пропозиція 5. Орграф $\Gamma(\rho) = (S, \rho)$ буде сильно зв'язним тоді і тільки тоді, коли кожна нетривіальна підмножина станів перетинається деякою дугою орграфу.

Означення 2. Орграф $\Gamma(\rho) = (S, \rho)$ назвемо ядерним, якщо $\gamma(\rho) = \zeta(\rho) = \varepsilon(\rho)$.

З рівності $\gamma(\rho) = \varepsilon(\rho)$ випливає, що кожна слабко зв'язна компонента ядерного орграфу $\Gamma(\rho)$ буде сильно зв'язною, тому ядерні орграфи є безпосереднім узагальненням сильно зв'язних орграфів.

Пропозиція 6. Орграф $\Gamma(\rho)$ буде ядерним тоді і тільки тоді, коли виконується одна з еквівалентних умов:

1) орграф $\Gamma(\rho)$ є об'єднанням сильно зв'язних компонент, між якими немає сполучних дуг орграфу;

2) через кожну дугу орграфу проходить деякий цикл.

Доведення. Якщо орграф $\Gamma(\rho)$ є ядерним, то кожна його слабко зв'язна компонента є сильно зв'язною, тому $\Gamma(\rho)$ буде об'єднанням своїх сильно зв'язних компонент, між якими немає сполучних дуг. Очевидно, що кожна нетривіальна дуга в сильно зв'язному орграфі міститься всередині деякого циклу. Отже, з ядерності графу випливає твердження 1, а із твердження 1 — твердження 2.

Якщо кожна дуга орграфу $\Gamma(\rho)$ міститься всередині деякого циклу, то $\zeta(\rho) = \zeta(\rho)^{-1}$. Тоді $\zeta(\rho)$ буде відношенням еквівалентності, тому $\gamma(\rho) = \zeta(\rho) = \varepsilon(\rho)$. Отже, орграф $\Gamma(\rho)$ буде ядерним і пропозицію доведено.

Відзначимо, що ядро скінченного автомата складається з незв'язних між собою сильно зв'язних підавтоматів, що і вмотивувало вибір термінології для орграфів.

Повернемося до груп переставлень. Позначимо $\mathrm{Aut}(S)$ повну симетричну групу всіх переставлень (бієкцій) на множині S. Групою переставлень G на множині S називається підгрупа $G \le \mathrm{Aut}(S)$ групи $\mathrm{Aut}(S)$. Група переставлень G діє на S природним чином, а саме, позначимо $g(s)$ образ стану s під дією переставлення $g \in G$. Стан t називається досяжним зі стану s у групі G, якщо існує переставлення $g \in G$ таке, що $g(s) = t$.

Відношення досяжності у групі є відношенням еквівалентності, оскільки воно симетричне, тому множина станів S розбивається на класи, які називаються орбітами групи G. Група переставлень G називається транзитивною, якщо для будь-якої пари станів s і t знайдеться переставлення $g \in G$ таке, що $g(s) = t$. Транзитивна група має одну орбіту, яка збігається з множиною S.

Дія групи переставлень G на множині S продовжується по компонентах на квадрат $S \times S$ за формулою $g(s, t) = (g(s), g(t))$ для $g \in G$. Пара станів (s_2, t_2) називається досяжною з пари (s_1, t_1) у групі G, якщо існує переставлення $g \in G$ таке, що $g(s_1, t_1) = (s_2, t_2)$. Це відношення досяжності також є відношенням еквівалентності; його класи еквівалентності (сильної зв'язності) називаються орбіталями групи G.

Нехай $\pi \subseteq S \times S$ — орбіталь групи переставлень G і $(s, t) \in \pi$, тоді виконується рівність

$$\pi = \{g(s, t) : g \in G\}. \tag{6}$$

Орбіталь називається нетривіальною, якщо вона складається з нетривіальних пар (s, t), де $s \ne t$. Якщо $\pi \subseteq (S \times S) \setminus \Delta_S$ — нетривіальна орбіталь групи переставлень G на множині S, то орграф $\Gamma(\pi) = (S, \pi)$ називається орбітальним орграфом цієї групи. Твердження, наведене далі, відоме з теорії груп переставлень [9].

Пропозиція 7. Орбітальний орграф транзитивної групи переставлень є ядерним.

Доведення. Нехай $\Gamma(\pi)=(S,\pi)$ — орбітальний орграф транзитивної групи переставлень $G \le \mathrm{Aut}(S)$ і $(s,t)\in\pi$. З огляду на транзитивність групи G знайдеться переставлення $g\in G$ таке, що $g(s)=t$. Тоді розглянемо дію циклічної групи $\langle g\rangle=\{e,g,\ldots,g^m\}$ на дугу (s,t). З формули (6) випливає, що послідовність станів $s, g(s),\ldots, g^m(s)$ утворює цикл в орграфі $\Gamma(\pi)$. Отже, через будь-яку дугу орграфу $\Gamma(\pi)$ проходить деякий цикл і згідно з пропозицією 6 орграф $\Gamma(\pi)$ буде ядерним. Пропозицію доведено.

ГРУПОВЕ ЗАМИКАННЯ ВІДНОШЕНЬ

Повернемося до загального випадку і розглянемо довільний спрямований ПІ-автомат $A=(S, I\cup Y, F)$ з нетривіальною групою переставлень $G(A)$. Групу $G(A)=F_A(Y^*)$ зобразимо як набір бієкцій за формулою $G(A)=\{g_w\colon w\in Y^*\}$, де $g_w(s)=F(s,w)$ для всіх $s\in S$, і вважатимемо базові бієкції g_y, $y\in Y$, бієкціями, що породжують групу $G(A)$.

Добутком (конкатенацією) двох наборів слів U і W називається набір $UW=\{u\in U, w\in W\}$, що складається з різноманітних добутків слів з цих наборів. Позначимо Y_m множину всіх групових слів, довжина яких менше, ніж m. З пропозиції 4 випливає, що в автоматі A існує збільшувальний набір слів вигляду IY_m для натурального числа m. Зважаючи на це, введемо таке означення.

Означення 3. ПІ-автомат $A=(S, I\cup Y, F)$ назвемо m-спрямованим, якщо набір слів IY_m є збільшувальним для A.

Для ПІ-автомата $A=(S, I\cup Y, F)$ визначимо ідемпотентне відношення $\rho_1=\{(h(x), t(x))\colon x\in I\}$ і відповідний орграф простих ідемпотентів $\Gamma_1=(S,\rho_1)$. Називатимемо пари, що входять до відношення ρ_1, ідемпотентними парами, а дуги орграфу Γ_1 — ідемпотентними дугами.

Нагадаємо, що група $G(A)$ діє на Декартовому квадраті $S\times S$ за компонентами $g_w(s,t)=(g_w(s), g_w(t))$ для $g_w\in G(A)$. Поширимо цю дію на ідемпотентне відношення ρ_1 і набір слів Y_m за формулою

$$\rho_m=\{g_w(s,t)\colon (s,t)\in\rho_1, w\in Y_m\}. \tag{7}$$

Отже, через включення $Y_m\subset Y_{m+1}$ для $m\ge 1$ отримуємо зростальний ланцюг відношень

$$\rho_1\subset\rho_2\subset\ldots\subset\rho_k=\rho_A. \tag{8}$$

Відношення ρ_m, $1\le m\le k$, що входить в ланцюг (8), називатимемо груповим m-замиканням відношення ρ_1. Відношення ρ_A, на якому обривається ланцюг (8), назвемо повним груповим замиканням відношення ρ_1. Зауважимо, що ланцюг (8) має обірватися принаймні через n^2-n кроків, де n — число станів автомата A.

З формули (7) випливає, що повне групове замикання відношення ρ_1 можна описати формулою

$$\rho_A=\{g_w(s,t)\colon (s,t)\in\rho_1, g_w\in G(A)\}. \tag{9}$$

Звідси і з формули (6) випливає, що відношення ρ_A є об'єднанням ідемпотентних орбіталей π_i, $1\le i\le d$, групи $G(A)$, тобто орбіталей, що містять принаймні одну ідемпотентну пару

$$\rho_A=\pi_1\cup\ldots\cup\pi_d. \tag{10}$$

Для доказу цієї рівності достатньо зазначити, що орбіталь π_i групи є повним груповим замиканням будь-якої пари $(s, t) \in \pi_i$. Групове m-замикання ідемпотентного відношення характеризує таке твердження [7].

Теорема 2. ПІ-автомат $A = (S, I \cup Y, F)$ буде m-спрямованим тоді і тільки тоді, коли орграф $\Gamma_m = (S, \rho_m)$ є сильно зв'язним.

Доведення. Нехай автомат A є m-спрямованим і IY_m — збільшувальний для нього набір слів, а T — нетривіальна підмножина станів, тоді для T існує збільшувальне слово вигляду xw, де $x \in I$ і $w \in Y^m$. Звідси випливає, що простий ідемпотент x буде збільшувальним для підмножини $U = g_w^{-1}(T) = F^{-1}(T, w)$, оскільки g_w є бієкцією і виконуються такі умови:

$$|F^{-1}(U, x)| = |F^{-1}(F^{-1}(T, w), x)| = |F^{-1}(T, xw)| > |T| = |U|.$$

Звідси і з пропозиції 3 випливає, що пара $(h(x),\ t(x))$ перетинає підмножину U, тобто $h(x) \notin U$ і $t(x) \in U$. Але тоді пара $g_w(h(x), t(x))$ буде перетинати підмножину T, оскільки $T = g_w(U)$ і g_w є бієкцією. Це означає, що для будь-якої нетривіальної підмножини T знайдеться дуга орграфу Γ_m, яка його перетинає. Тоді згідно з пропозицією 5 орграф Γ_m буде сильно зв'язним.

Навпаки, нехай орграф Γ_m є сильно зв'язним і T — нетривіальна підмножина станів. Тоді згідно з пропозицією 5 підмножина T перетинається деякою дугою $g_w(h(x), t(x))$ орграфу Γ_m. У цьому разі дуга $(h(x),\ t(x))$ буде перетинати підмножину $U = g_w^{-1}(T)$. Тоді згідно з пропозицією 3 дійдемо висновку, що символ x буде збільшувальним для U, отже, слово xw буде збільшувальним для T. Таким чином, автомат A буде m-спрямованим.

Теорему доведено.

З теореми 2 як наслідок отримуємо таке твердження.

Наслідок 1. ПІ-автомат $A = (S, I \cup Y, F)$ буде спрямованим тоді і тільки тоді, коли орграф $\Gamma_A = (S, \rho_A)$ є сильно зв'язним.

Особливий інтерес становить n-замикання ρ_n ідемпотентного відношення, де n — число станів автомата A. Якщо орграф $\Gamma_n = (S, \rho_n)$ буде сильно зв'язним, то за теоремою 2 автомат A буде n-спрямованим і, отже, згідно з пропозицією 2 для нього буде виконуватись гіпотеза Черні. З огляду на це розглянемо такий клас груп.

Група переставлень G на множині S називається регулярною, якщо для будь-якої пари станів $(s,\ t)$ існує тільки одне переставлення $g \in G$ таке, що $g(s) = t$. Звідси випливає, що регулярна група переставлень ступеня $n = |S|$ складається точно з n переставлень $G = \{e, g_1, \ldots, g_{n-1}\}$. Отже, для будь-якої системи породжувальних H групи G кожен її неодиничний елемент породжується ланцюжком довжини не більше ніж $n-1$, що можна записати у такому вигляді:

$$G = \{e\} \cup H \cup \ldots \cup H^{n-1}. \tag{11}$$

Звідси отримуємо основний результат.

Теорема 3. Нехай $A = (S, I \cup Y, F)$ — спрямований ПІ-автомат з n станами і регулярною групою, тоді $C(A) \le (n-1)^2$.

Доведення. Оскільки автомат A є спрямованим, то згідно з наслідком 1 його орграф $\Gamma_A = (S, \rho_A)$ буде сильно зв'язним. Але з формул (7), (9) та (11) випливає, що для автомата з регулярною групою виконується рівність

$$\rho_n = \{g_w(s, t) : (s, t) \in \rho_1,\ w \in Y_n\} = \rho_A.$$

Отже, орграф $\Gamma_n = (S, \rho_n)$ також буде сильно зв'язним і за теоремою 2 автомат A є n-спрямованим. Звідси і з пропозиції 2 випливає нерівність $C(A) \le (n-1)^2$.

Теорему доведено.

Зауважимо, що клас автоматів, зазначений в теоремі 3, є безпосереднім узагальненням серії автоматів Черні [1], які є спрямованими ПІ-автоматами з одним простим ідемпотентом і регулярною (циклічною) групою. Вони мають одну ідемпотентну орбіталь, яка є циклом, що проходить через всі стани автомата.

Узагальнення цього результату на транзитивні групи має певні труднощі [10]. Крім того, у праці [10] розглядаються автомати з незвідною групою (над полем раціональних чисел Q). Як наслідок цієї роботи отримуємо таке твердження.

Теорема 4. Нехай $A = (S, X, F)$ — спрямований автомат з n станами і регулярною незвідною групою, тоді $C(A) \le (n-1)^2$.

У порівнянні з теоремою 3 тут послаблена умова, що накладається на сингуляри, тобто на морфізми, які не є бієкціями, але посилено умову, що накладається на групу автомата. Цікаво відзначити, що теорема 4 є безпосереднім узагальненням результату Пена [2].

СПИСОК ЛІТЕРАТУРИ

1. Černy J. Poznamka k homogennym experimentom s konecnymy automatami. *Math. Fyz. Cas. SAV*. 1964. Vol. 14. P. 208–215.
2. Pin E. Sur un cas particulier de la conjecture de Cerny. *Lecture Notes in Computer Science*. 1978. Vol. 62. P. 345–352.
3. Eppstein D. Reset sequences for monotonic automata. *SIAM J. Computer*. 1990. Vol. 19, N 3. P. 500–510.
4. Dubuc L. Sur les automates circulaires et la conjecture de Cerny. *RAIRO-Theor. Inf. Appl*. 1998. Vol. 32, N 1–3. P. 21–34.
5. Steinberg B. The Cerny conjecture for one-cluster automata with prime length cycle. *Theoretical Computer Sci*. 2011. Vol. 412, N 39. P. 5487–5491.
6. Рысцов И.К. Почти оптимальная оценка длины возвратного слова для регулярных автоматов. *Кибернетика и системный анализ*. 1995. Т. 31, № 5. С. 40–47.
7. Рысцов И.К. О длине возвратных слов для автоматов с простыми идемпотентами. *Кибернетика и системный анализ*. 2000. Т. 36, № 3. С. 32–39.
8. Рисцов І.К. Застосування методів алгебраїчної теорії автоматів к проблемам аналізу дискретних динамічних систем: дис. … д-ра фіз.-мат. наук. Київ: Київ. нац. ун-т, 2020. 301 с.
9. Баннаи Э., Ито Т. Алгебраическая комбинаторика. Схемы отношений. Москва: Мир, 1987. 375 с.
10. Steinberg B. Černy's conjecture and group representation theory. URL: http://arxiv.org/pdf/0808.1429.pdf. Accessed on: 10 Aug. 2008.

I.K. Rystsov

ON THE CERNY PROBLEM FOR AUTOMATA WITH SIMPLE IDEMPOTENTS

Abstract. In this paper, two tight bounds of the Cherny function $C(A)$ are obtained for automata with simple idempotents (SI-automata). It is shown that $C(A) = n-1$ for the SI-automaton A with n states and a trivial group and $C(A) \le (n-1)^2$ for the SI-automaton A with n states and a regular group.

Keywords: finite automata, Cerny's conjecture.

Надійшла до редакції 26.08.2021