MATHEMATICAL AND COMPUTER MODELING

DOI 10.20535/2411-1031.2024.12.1.306274
УДК 004.75

ОКСАНА КУБАЙЧУК,
ДЕНИС САЙ

РАНДОМІЗОВАНІ АЛГОРИТМИ В СИСТЕМАХ БЕЗ КООРДИНАЦІЇ ТА ЦЕНТРАЛІЗАЦІЇ

Оцінювання складності алгоритмів виходячи тільки з можливості найгіршого варіанту вхідних даних є часто не виправданим. Розробка алгоритмів, які б очікувано швидко працювали на всіх можливих входах має практичне значення. Якщо для задачі існує розумна можливість змоделювати розподіли вхідних величин, то можна скористатися ймовірнісним аналізом як методом розробки ефективних алгоритмів. Коли ж інформації про розподіли вхідних величин недостатньо для їх чисельного моделювання, розробляють алгоритми шляхом надання випадкового характеру частині самого алгоритму – рандомізовані алгоритми.

Застосування рандомізації забезпечує функціонування алгоритму при мінімальних потребах у зберіганні внутрішніх станів та подій у минулому, причому самі алгоритми виглядають компактно.

В роботі вивчаються задачі, для яких існують відносно ефективні детерміновані алгоритми розв’язання. Але, як буде показано, побудова відповідних рандомізованих алгоритмів призводить до ефектних та ефективних схем паралельних обчислень з лінійною складністю в середньому. Переваги рандомізації особливо проявляються у випадку великих комп’ютерних систем та комунікаційних мереж, які функціонують без координації та централізації. Прикладами таких розподілених систем є, зокрема, мережі популярних нині криптовалют. Застосування рандомізованих евристик дозволяє системі адаптуватися до змінних умов експлуатації та мінімізує ймовірність конфліктів між процесами.

В роботі показано переваги застосування рандомізованого алгоритму перед детермінованими алгоритмами для задачі маршрутизації в мережі з топологією гіперкуба. Доведено теорему про оцінку очікуваного числа кроків, необхідних рандомізованому алгоритму Валіанта для доставки всіх повідомлень за адресою. Очікувана лінійна складність алгоритму Валіанта є прямим наслідком доведеної теореми.

Ключові слова: рандомізований алгоритм, паралельні обчислення, ймовірнісний аналіз, складність в середньому, нерівності Чернова-Хеффдінга, нерівність Маркова, маршрутизація в гіперкубі.

Вступ. Підхід до оцінювання складності алгоритмів виходячи з можливості найгіршого варіанту вхідних даних є часто не виправданим. Розробка таких алгоритмів, які б очікувано (в середньому) швидко працювали на всіх можливих входах має практичне значення. Для деяких задач можливо зробити розумні припущення про розподіли вхідних величин і скористатися ймовірнісним аналізом як методом розробки ефективних алгоритмів. Коли ж інформації про розподіли вхідних величин недостатньо для їх чисельного моделювання, розробляють алгоритми шляхом надання випадкового характеру частині самого алгоритму – рандомізовані алгоритми.

В загальному випадку алгоритм є рандомізованим, якщо його поведінка залежить, у тому числі, від значень, згенерованих датчиком випадкових чисел. На практиці розробники алгоритмів використовують датчики псевдовипадкових чисел – детерміновані алгоритми, що генерують послідовності чисел, які задовольняють деякий набір статистичних тестів.

Очевидно, що навіть у випадку фіксованого входу час роботи рандомізованого алгоритму є випадковою величиною.

В роботі розглядаються задачі, для яких відомі відносно ефективні детерміновані алгоритми розв'язання. Але навіть у цьому випадку застосування рандомізації забезпечує функціонування алгоритму при мінімальних потребах у зберіганні внутрішніх станів та подій у минулому, причому самі алгоритми виглядають компактно. Переваги рандомізації особливо проявляються при розгляді великих комп'ютерних систем та комунікаційних мереж, зокрема, у системах без координації та централізації – розподілених системах. Застосування рандомізованих евристик дозволяє системі адаптуватися до змінних умов експлуатації, знижуючи ймовірність конфліктів між процесами.

Аналіз останніх досліджень та публікацій. Потужні рандомізовані алгоритми розв'язання складних задач теорії чисел розроблено в 70-х роках минулого століття. Яскравими прикладами є рандомізовані тести на простоту Соловея-Штрассена та Рабіна. Відтоді, рандомізація стає потужним інструментом для розробки широкого кола застосунків, а теми рандомізації та ймовірнісного аналізу є невід'ємною частиною комп'ютерної науки.

Вирішення конфліктів шляхом застосування рандомізації є типовим для різних систем. Наприклад, в комунікаційних мережах рандомізовані протоколи використовуються задля мінімізації колізій між різними відправниками.

Рандомізований алгоритм розроблений Штайном та Каргером на даний момент є дним з найкращих алгоритмів розв'язання задачі про мінімальний розріз [1]. Метод Штайна та Каргера береться за основу багатьма дослідниками, наприклад, [2].

Рандомізація довела свою ефективність при розробці спеціалізованих структур даних. Застосування рандомізваних хеш-функцій є ефективним способом організації зберігання множини об'єктів, яка інтенсивно змінюється. Прикладом є рандомізована реалізація словників [3]. За умови адекватного вибору рандомізованої хеш-функції, алгоритм Рабіна-Карпа [4] успішно використовується в додатках перевірки на плагіат.

У роботах [5] і [6] показано, що детерміновані алгоритми маршрутизації з відсутністю післядії в мережі з топологією гіперкуба мають експоненційну складність. Поліноміальну складність пакетної маршрутизації в контексті довжини максимального шляху та максимального навантаження доведено в [7]. Валіантом в [8] запропоновано рандомізований алгоритм маршрутизації, який використовував схему виправлення бітів, а у [9] емпіричним шляхом здобуто ооцінки для деяких параметрів алгоритму для мережі з топологією гіперкуба. Проблему маршрутизації для мереж зі складнішими топологіями розглянуто, зокрема, у роботах Ракке [10], [11]. Для її розв'язання автором застосовуються методи системного аналізу та теорії графів у поєднанні з рандомізованими евристиками.

Рандомізовані евристики широко застосовуються в задачах криптоаналізу. Серед останніх робіт у цьому напрямку можна відзначити роботи [12]–[17]. Особливості застосування алгоритму ACO розглянуто в [18]. Детальний огляд результатів метаевристичного підходу до розв'язання задач криптогафічного аналізу є у роботі [19].

Мета дослідження. Уточнити та навести строгі доведення результатів здобутих у роботах [20], [21]. Оцінити знизу число повторних запусків рандомізованого алгоритму, щоб ймовірність помилкового розв'язання задачі була не більше за наперед вибране $\varepsilon > 0$. Показати переваги рандомізованих алгоритмів у порівнянні з детермінованими.

Виклад основного матеріалу дослідження. Перетворення Фур'є застосовується в багатьох розділах математики. У теорії ймовірностей це інтегральне перетворення відоме як характеристична функція.

Нехай ξ – випадкова величина, а F – її функція розподілу. Характеристичною функцією випадкової величини ξ та функції розподілу F називається така комплекснозначна функція дійсної змінної t:

$$\varphi_\xi(t) \equiv Me^{it\xi} = \int_{-\infty}^{\infty} e^{it\xi} dF(x) \equiv \varphi_F(t).$$

Поряд з характеристичною функцією застосовують і інші інтегральні перетворення, зокрема, твірну функцію моментів.

Твірною функцією моментів випадкової величини ξ називається функція змінної t:

$$m_\xi(t) \equiv Me^{t\xi}$$

у припущенні, що величина під знаком математичного сподівання інтегровна для всіх t з деякого околу нуля.

Твірна функція моментів розкладається в ряд Тейлора

$$m_\xi(t) = \sum_{n\geq 0} t^n M\xi^n / n!$$

звідки, наприклад,

$$M\xi^n = m_\xi^{(n)}(0),\ n>1,$$

за умови, що інтеграли існують.

Нерівність Маркова. Нехай ξ – випадкова величина, що приймає невід'ємні значення. Тоді, $\forall\ a>0$:

$$\Pr\{\xi \geq a\} \leq \frac{M\xi}{a}.$$

Користуючись нерівністю Маркова, для будь-якого $t>0$, маємо:

$$\Pr\{\xi \geq a\} = \Pr\left\{e^{t\xi} \geq e^{ta}\right\} \leq \frac{Me^{t\xi}}{e^{ta}} = \frac{m_\xi(t)}{e^{ta}}.$$

І, аналогічно, для будь-якого $t<0$

$$\Pr\{\xi \leq a\} = \Pr\left\{e^{t\xi} \geq e^{ta}\right\} \leq \frac{Me^{t\xi}}{e^{ta}} = \frac{m_\xi(t)}{e^{ta}}.$$

Далі, розглянемо випадкову величину $S_n = \xi_1 + \ldots + \xi_n$, де $\xi_i, 1 \leq i \leq n$ – незалежні у сукупності випадкові величини, що мають розподіл Бернуллі з ймовірністю успіху p_i, відповідно. Тоді,

$$\mu = MS_n = \sum_{i=1}^n M\xi_i = \sum_{i=1}^n p_i.$$

Нерівності Чернова-Хеффдінга – це оцінки ймовірності істотного відхилення S_n від MS_n, які випливають з нерівності Маркова. Зокрема, для $\delta>0$ розглядають ймовірності

$$\Pr\{S_n \geq (1+\delta)\mu\}$$

і

$$\Pr\{S_n \leq (1-\delta)\mu\}.$$

Теорема *(нерівності Чернова-Хеффдінга*). Нехай S_n – випадкова величина, визначена вище. Істинними є наступні нерівності:

1. $\forall\delta>0,\ \Pr\{S_n \geq (1+\delta)\mu\} \leq \left(\frac{e^\delta}{(1+\delta)^{(1+\delta)}}\right)^\mu$;
2. $0<\delta\leq 1,\ \Pr\{S_n \geq (1+\delta)\mu\} \leq e^{-\mu\delta^2/3}$;
3. $\theta \geq 6\mu,\ \Pr\{S_n \geq \theta\} \leq 2^{-\theta}$;
4. $0<\delta<1,\ \Pr\{S_n \leq (1-\delta)\mu\} \leq \left(\frac{e^\delta}{(1-\delta)^{(1-\delta)}}\right)^\mu$;
5. $0<\delta<1,\ \Pr\{S_n \leq (1-\delta)\mu\} \leq e^{-\mu\delta^2/2}$.

Зниження ймовірності помилки. Припустимо, що алгоритм знаходить існуючий розв'язок з ймовірністю p.

Задача. Оцінити знизу число повторних запусків цього алгоритму, щоб ймовірність помилкового розв'язання була не більше за наперед вибране $\varepsilon > 0$.

Розв'язання. Ймовірність неуспіху алгоритму $1-p$. Тому, $t_0 = t(\varepsilon)$ – число повторень алгоритму, має задовольняти нерівність:

$$(1-p)^{t_0} \le \varepsilon .$$

$$t_0 \ln(1-p) \le \ln\varepsilon \Leftrightarrow t_0 \ln\left(1+\frac{p}{1-p}\right) \ge \ln\frac{1}{\varepsilon} \Leftrightarrow$$

$$t_0\left(\frac{p}{1-p}\right) \ge \ln\frac{1}{\varepsilon} \Leftrightarrow t_0 \ge \left(\frac{1-p}{p}\right)\ln\frac{1}{\varepsilon}$$

Тобто, алгоритмом, який видає правилну відповідь з малою ймовірністю можна скористатись, повторно запускаючи його принаймні t_0 раз.

Маршрутизація в гіперкубі. Розглядається комунікаційна мережа з n вузлів, кожен з яких є відправником і отримувачем точно одного з n повідомлень. Потрібно доставити кожне повідомлення за призначенням якнайшвидше.

Кожен вузол має унікальну адресу, а мережа працює синхронно, кроками. На кожному кроці: кожне повідомлення рухається тільки по одному ребру, або залишається в черзі вузла; кожне ребро переносить не більше одного повідомлення.

Припускається, що моделлю мережі є розріджений граф з топологією гіперкуба. Тобто, мережа складається з $n = 2^m$ вузлів, де m – бітова розрядність адреси вузла (*розмірність, діаметр* гіперкуба). Ребро між двома вузлами існує тоді й тільки тоді, коли їхні адреси відрізняються рівно одним бітом.

До гіперкубу застосовна схема маршрутизації за якою, повідомлення, що знаходиться у вузлі з адресою $\beta = (\beta_1, \beta_2, \ldots \beta_m)$ та цільовою адресою $\alpha = (\alpha_1, \alpha_2, \ldots \alpha_m)$, відправляється по ребру, що відповідає найменшому i такому, що $\alpha_i \ne \beta_i$. Таку схему називають *схемою виправлення бітів* (Bit-Fixing Routing Algorithm):

Нехай a і b адреси відправника та отримувача пакета, відповідно.

For $i = 1$ to n, do

If $\alpha_i \ne \beta_i$ move $(b_1 \ldots b_{i-1} a_i \ldots a_n) \to (b_1 \ldots b_{i-1} b_i a_{i+1} \ldots a_n)$.

Наприклад, повідомлення 3 000 у 111 піде за маршрутом:

$$000 \to 100 \to 110 \to 111.$$

Нижня оцінка числа кроків. Для схем маршрутизації з відсутністю післядії належить схема виправлення бітів (маршрут повідомлення повністю визначається адресами відправника та одержувача). У роботі [5] доведено *нижню* асимптотичну оцінку складності для будь-якого детермінованого алгоритму з відсутністю післядії – $\Omega(\sqrt{n}/d^{3/2})$, де d – діаметр мережі. Оцінка в наших позначеннях для мережі з топологією гіперкуба матиме вигляд $\Omega(\sqrt{2^m}/m^{3/2})$, або ж більш грубо $\Omega(\sqrt{2^m/m})$, що, доречі показано у [6]. Тобто, детермінований алгоритм з відсутністю післядії має експоненційну складність.

Рандомізований алгоритм. Пропонується розглянути рандомізований алгоритм Валіанта доставки всіх 2^m повідомлень за призначенням [8]. Алгоритм регулює навантаження на мережу, скорочуючи черги у вузлах. Пришвидшити його практично неможливо, оскільки діаметр гіперкуба m.

Алгоритм *(Валіант)*

Використовуючи схему виправлення бітів:

(А) Доставити кожне повідомлення i на випадкову адресу $r(i)$.

(Б) Доставити кожне повідомлення i з $r(i)$ за призначенням.

Псевдокод алгоритму.

Позначення. Нехай, $V=\{0,1,2,\ldots,n-1\}$ множина 2^m вершин m-вимірного куба. Для $i\in\{1,2,\ldots,m\}$ і $x\in V$ позначення x^i означає i-тий найбільш значущий біт у m-бітовому представленні числа x. Позначення $x\updownarrow i$ означає число, що отримується з x заміною i-того біта на протилежний. Отже, множину $m2^m$ ребер, що з'єднують вершини з V можна подати як $E=\{(x,x\updownarrow i): x\in V,\ i\in\{1,\ldots m\}\}$. Для кожного такого ребра існує черга $Q(x,i)$, що живить його з вершини x. Для кожного вузла x підтримується множина пакетів у ньому L_x. Запис $rund\,\alpha\in$ A означає випадковий вибір елемента з множини A та присвоєння його значення змінній α. Скажемо, що фазу завершено, якщо $\forall v\in V:\ T_v=\varnothing$, де $T_v\subseteq\{1,\ldots,n\}$.

Фаза (А)
For $x\in V$ do $L_x=\{x\}$
$T_x=\{1,\ldots,n\}$
For $j=1$ until F do
For $x\in V$ do if $L_x\neq\varnothing$ then for
Each $v\in L_x$ with $T_v\neq\varnothing$ do
Begin $rund\,i\in T_v$
$T_v=T_v-\{i\}$
$rund\,\alpha\in\{0,1\}$
If $\alpha=1$ then
Begin add v to $Q(x,i)$
$L_x=L_x-\{v\}$
End begin
End begin
Transmit x
Фаза (Б)
For $x\in V$ do if packet with address x is at node u
Then $T_x=\{i: x^i\neq u^i\}$
For $k=1$ until G do
For $u\in V$ do if $L_u\neq\varnothing$ then for
Each $v\in L_u$ with $T_v\neq\varnothing$ do
Begin $L_u=L_u-\{v\}$
$rund\,i\in T_v$
$T_v=T_v-\{i\}$
add v to $Q(u,i)$
End begin
Transmit u

Розглянемо випадкову величину ξ – число кроків для доставки всіх 2^m пакетів (повідомлень) за призначенням алгоритмом Валіанта. Побудуємо оцінку для $M\xi$.

Число кроків для доставки повідомлення i на випадкову адресу $r(i)$ складається з числа кроків *в дорозі* від вузла до вузла, пройдених повідомленням i на шляху до $r(i)$, і тих

кроків, коли повідомлення i перебувало *в чергах*. Число кроків в дорозі обмежено зверху m – діаметром гіперкуба. Далі, оцінимо число кроків алгоритму у чергах.

Нехай $t_i = (e_1, e_2, \ldots e_k)$ – маршрут (трек) повідомлення i на шляху до $r(i)$, з $k \le m$ ребер. Для пари повідомлень i та j розглянемо індикатор події { t_i та t_j мають спільні ребра }:

$$I_{ij} = \begin{cases} 1, & t_i \cap t_j \neq \varnothing \\ 0, & \text{otherwize} \end{cases}.$$

Далі, для повідомлення i розглянемо множину повідомлень, які на своєму шляху використовують ребра з t_i:

$$\Delta_i \doteq \{ j : j \neq i,\ I_{ij} = 1 \}$$

В лемі 4.5 з [20] доводиться, що число кроків, проведених повідомленням i в чергах не перевищує $|\Delta_i|$.

Твердження 1. $M|\Delta_i| \le m$.

Доведення. Розглянемо випадкову величину $T(e)$ – число повідомлень, які використовують ребро e гіперкуба на кроці алгоритму з деякою ймовірністю p,

$$T(e) = \begin{cases} 1, & p \\ 0, & 1-p \end{cases};$$

$$M[T(e)] = p \le 1.$$

$$|\Delta_i| = \sum_{j \neq i} I_{ij} = \sum_{l=1}^{k} \sum_{j \neq l} I_{lj}.$$

Тоді

$$M|\Delta_i| = \sum_{l=1}^{k} M\left[\sum_{j \neq l} I_{lj}\right] = \sum_{l=1}^{k} M[T(e_l)] \le \sum_{l=1}^{m} M[T(e_l)].$$

Остаточно, $M|\Delta_i| \le m$. Твердження 1 доведено.

Твердження 2. $\Pr\{\xi \le 14m\} \ge 1 - 2^{-4m}$.

Доведення. Для будь-якого повідомлення i, випадкові величини I_{ij} для різних j незалежні. За нерівністю Чернова-Хеффдінга у формі (3), враховуючи твердження 1, маємо

$$\Pr\{|\Delta_i| \ge 6m\} \le 2^{-6m}.$$

Нехай $A_i = \{ i$ проводить в черзі не менше $6m$ кроків$\}$. Враховуючи лему 4.5 з [20], маємо $\{|\Delta_i| \ge 6m\} \supseteq A_i$. Звідси,

$$\Pr\{A_i\} \le 2^{-6m}.$$

З нерівності Буля

$$\Pr\left\{\bigcup_{i=1}^{n} A_i\right\} \le \sum_{i=1}^{n} \Pr\{A_i\},$$

яка є істинною для будь-яких подій $A_1, \ldots, A_n$, враховуючи, що число всіх повідомлень дорівнює 2^m, маємо:

$$\Pr\left\{\bigcup_{i=1}^{2^m} A_i\right\} \le 2^m \cdot 2^{-6m} = 2^{-5m}.$$

Тобто, ймовірність того, хоча б одне повідомлення проведе в чергах більше ніж $6m$ кроків не перевищує 2^{-5m}. Отже, доставка всіх повідомлень на випадкову адресу (фаза (А)

алгоритму Валіанта), враховуючи рух по ребрах (в дорозі) займе більше ніж $7m$ кроків з ймовірністю не більше ніж 2^{-5m}.

Викладки для фази (Б) алгоритму Валіанта аналогічні. Тому, доставка всіх повідомлень за заданою адресою займе більше ніж $14m$ кроків з ймовірністю не більше $2\cdot 2^{-5m}$:

$$\Pr\{\xi > 14m\} \le 2^{-5m+1}.$$

Звідси,

$$\Pr\{\xi \le 14m\} \ge 1-2^{-5m+1} \ge 1-2^{-5m+m} = 1-2^{-4m}.$$

Твердження 2 доведено.

Теорема 1. Нехай випадкова величина ξ – число кроків, необхідних алгоритму Валіанта для доставки всіх пакетів за призначенням. Тоді $\exists L>0$ таке, що $M\xi \le Lm$, де m – бітова розрядність адреси вузла.

Доведення. Очевидно, випадкова величина ξ може приймати значення не більші ніж $2^m \cdot m$, оскільки кожне з 2^m повідомлень можна доставити по m ребрам незалежно від інших. Отже,

$$M\xi = \sum_i i\cdot \Pr\{\xi = i\} = \sum_{i\le 14m} i\cdot \Pr\{\xi = i\} + \sum_{i>14m} i\cdot P\{\xi = i\} \le$$
$$\le 14m \sum_{i\le 14m} \Pr\{\xi = i\} + m\cdot 2^m \sum_{i>14m} \Pr\{\xi = i\} \le$$
$$\le 14m \Pr\{\xi \le 14m\} + m2^m \Pr\{\xi > 14m\}$$

Далі, застосовуючи твердження 2, отримаємо оцінку зверху ймовірності протилежної події

$$\Pr\{\xi > 14m\} \le 1-\left(1-2^{-4m}\right).$$

Отже,

$$M\xi \le 14m\cdot 1 + m2^m \cdot \left(1-(1-2^{-4m})\right) =$$
$$= 14m + m2^{-3m} = \left(14+2^{-3m}\right)m$$

.

Очевидно, за L можна обрати значення $14+2^{-3} \approx 14{,}125 > 0$. Теорему 1 доведено.

Моделювання значення L на (див. рис. 1) у середовищі Mathcad v.13.

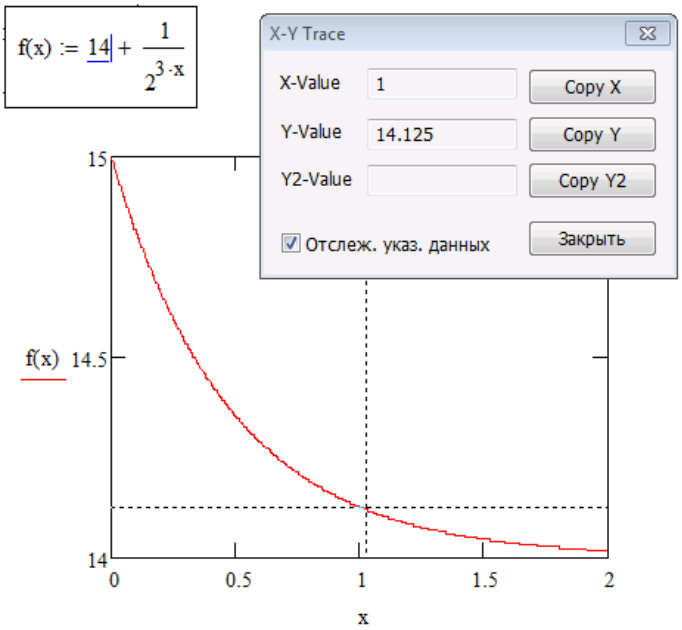

Рисунок 1 – Про вибір L

Наслідок 1. За означенням відношення "O" складність алгоритму Валіанта $O(m)$ в середньому.

Висновки. У роботі уточнено формулювання та наведено строгі доведення деяких результатів здобутих у роботах [20], [21], показано переваги застосування рандомізованого алгоритму, який оптимізує розподіл навантаження у мережі, перед детермінованими алгоритмами для задачі маршрутизації. Для мережі з топологією гіперкуба доведено теорему про оцінку зверху математичного сподівання випадкової величини – число кроків, необхідних рандомізованому алгоритму Валіанта для доставки всіх повідомлень за адресою за схемою виправлення бітів. Наслідком доведеної теореми є твердження, що складність алгоритму Валіанта є $O(m)$ в середньому, де m – бітова розрядність адреси вузла. Показано, як повторні запуски рандомізованого алгоритму приводять до зменшення ймовірності помилкового результату. А саме, здобуто оцінку знизу числа повторних запусків, необхідних для того, щоб ймовірність помилкового розв'язання знаходилась у наперед заданих межах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] D.R. Karger, and C. Stein, "A new approach to the minimum cut problem", *Journal of the ACM (JACM)*, vol. 43, iss. 4, 601-640, 1966.

[2] A. Gupta, E. Lee, and J. Li, "The number of minimum k-cuts: Improving the Karger-Stein bound". in *Proc. 51st Annual ACM SIGACT Symposium on Theory of Computing*, 2019, pp. 229-240, doi: https://doi.org/10.48550/arXiv.1906.00417.

[3] M.N. Wegman, and J.L. Carter, "New hash functions and their use in authentication and set equality", *J. Comput. System Sci*, vol. 22, pp. 265-279, 1981.

[4] M.O. Rabin, and R.M. Karp, "Efficient randomized pattern-matching algorithms", *IBM Journal of Research and Development*, vol. 31, no. 2, pp. 249-260, 1987, doi: https://doi.org/10.1147/rd.312.0249.

[5] A. Borodin, and J.E. Hopcroft, "Routing, merging, and sorting on parallel models of computation", *Journal of Computer and System Sciences*, vol. 30 (1), pp. 130-145, 1985, doi: https://doi.org/10.1016/0022-0000(85)90008-X.

[6] C. Kaklamanis, D. Krizanc, and T. Tsantilas, "Tight bounds for oblivious routing in the hypercube", *Mathematical Systems Theory*, vol. 24 (4), pp. 223-232, 1991, doi: https://doi.org/10.1007/BF02090400.

[7] F.T. Leighton, B.M. Maggs, and S.B. Rao, "Packet routing and job-shop scheduling in$O$(congestion+dilation) steps", *Combinatorica*, vol. 14, pp. 167-186, 1994, doi: https://doi.org/10.1007/BF01215349.

[8] L.G. Valiant, and G.J. Brebner, "Universal schemes for parallel communication", in *Proc. 13th Ann. ACM Symp. on Theory of Comp*. (*STOC'81)*, 1981, pp. 263-277, 1981, doi: https://doi.org/10.1145/800076.802479.

[9] L.G. Valiant, "A scheme for fast parallel communication", *SIAM Journal on Computing*, iss. 11 (2), pp. 350-361, 1982, doi: https://doi.org/10.1137/0211027.

[10] H. Räcke, and S. Schmid, "Compact oblivious routing", in *Proc. 27th Europ. Symp. on Algor. (ESA 2019), Leibniz Int. Proc. in Inform. (LIPIcs)*, Schloss Dagstuhl, 2019, vol. 144, pp. 75:1-75:14, doi: https://doi.org/10.4230/LIPIcs.ESA.2019.75.

[11] P. Czerner, and H. Räcke, "Compact Oblivious Routing in Weighted Graphs", in *Proc. 28th Ann. Europ. Symp. on Algor. (ESA 2020), Leibniz Int. Proc. in Inform. (LIPIcs)*, Schloss Dagstuhl, 2020, vol. 173, pp. 36:1-36:23, doi: https://doi.org/10.4230/LIPIcs.ESA.2020.36.

[12] D. Rachmawati, H. Tamara, S. Sembiring, and M. Budiman, “RSA public key solving technique by using genetic algorithm”, *Journal of Theoretical and Applied Information Technology*, vol. 98, iss. 15, pp. 2990-2999, 2020.

[13] A.K.S. Sabonchi, and B. Akay, “Cryptanalysis of polyalphabetic cipher using differential evolution algorithm”, *Tehnički vjesnik*, iss. 27 (4), pp. 1101-1107, 2020, doi: https://doi.org/10.17559/TV-20190314095054.

[14] B. Akay, “A binomial crossover based artificial bee colony algorithm for cryptanalysis of polyalphabetic cipher”, *Tehnički vjesnik*, iss. 27 (6). pp. 1825-1835, 2020, doi: https://doi.org/10.17559/TV-20190422225110.

[15] A.K.S. Sabonchi, B. Akay, “A survey on the Metaheuristics for Cryptanalysis of Substitution and Transposition Ciphers”, *Computer Systems Science And Engineering*, vol. 39, no. 1, pp. 87-106, 2021, doi: http://doi.org/10.32604/csse.2021.05365.

[16] H. Grari, S. Lamzabi, A. Azouaoui, and K. Zine-Dine, “Cryptanalysis of Merkle-Hellman cipher using ant colony optimization”, *Int. Jour. Artif. Intell. (IJ-AI)*, vol. 10, no. 2, pp. 490-500, 2021, doi: https://doi.org/10.11591/ijai.v10.i2.

[17] K. Dworak, and U. Boryczka, “Breaking Data Encryption Standard with a Reduced Number of Rounds Using Metaheuristics Differential Cryptanalysis”, *Entropy*. vol. 23, iss. 12, pp. 1697-1718, 2021, doi: https://doi.org/10.3390/e23121697.

[18] О.О. Кубайчук, “Особливості застосування алгоритму ACO до деяких задач криптоаналізу”, *Наукоємні технології,* № 2 (58), с. 141-148, 2023, doi: https://doi.org/10.18372/2310-5461.58.17650.

[19] О.О. Кубайчук, “Огляд застосування метаевристичного підходу в криптоаналізі”, *Вісник ХНТУ: інформаційні технології,* № 2 (85), с. 147-153, 2023, doi: https://doi.org/10.35546/kntu2078-4481.2023.2.20.

[20] R. Motwani, and P. Raghavan, *Randomized Algorithms*. Cambridge, GB: Cambridge Univ. Press, 1995.

[21] M. Mitzenmacher, and E.Upfal, *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. Cambridge, GB: Cambridge Univ. Press, 2005.

Стаття надійшла до редакції 14.05.2024

REFERENCE

[1] D.R. Karger, and C. Stein, “A new approach to the minimum cut problem”, *Journal of the ACM (JACM)*, vol. 43, iss. 4, 601-640, 1966.

[2] Gupta, E. Lee, and J. Li, “The number of minimum k-cuts: Improving the Karger-Stein bound”. in *Proc. 51st Annual ACM SIGACT Symposium on Theory of Computing*, 2019, pp. 229-240, doi: https://doi.org/10.48550/arXiv.1906.00417.

[3] M.N. Wegman, and J.L. Carter, “New hash functions and their use in authentication and set equality”, *J. Comput. System Sci*, vol. 22, pp. 265-279, 1981.

[4] M.O. Rabin, and R.M. Karp, “Efficient randomized pattern-matching algorithms”, *IBM Journal of Research and Development*, vol. 31, no. 2, pp. 249-260, 1987, doi: https://doi.org/10.1147/rd.312.0249.

[5] Borodin, and J.E. Hopcroft, “Routing, merging, and sorting on parallel models of computation”, *Journal of Computer and System Sciences*, vol. 30 (1), pp. 130-145, 1985, doi: https://doi.org/10.1016/0022-0000(85)90008-X.

[6] C. Kaklamanis, D. Krizanc, and T. Tsantilas, “Tight bounds for oblivious routing in the hypercube”, *Mathematical Systems Theory*, vol. 24 (4), pp. 223-232, 1991, doi: https://doi.org/10.1007/BF02090400.

[7] F.T. Leighton, B.M. Maggs, and S.B. Rao, “Packet routing and job-shop scheduling in*O*(congestion+dilation) steps”, *Combinatorica*, vol. 14, pp. 167-186, 1994, doi: https://doi.org/10.1007/BF01215349.

[8] L.G. Valiant, and G.J. Brebner, “Universal schemes for parallel communication”, in *Proc. 13th Ann. ACM Symp. on Theory of Comp*. (*STOC’81)*, 1981, pp. 263-277, 1981, doi: https://doi.org/10.1145/800076.802479.

[9] L.G. Valiant, “A scheme for fast parallel communication”, *SIAM Journal on Computing*, iss. 11 (2), pp. 350-361, 1982, doi: https://doi.org/10.1137/0211027.

[10] H. Räcke, and S. Schmid, “Compact oblivious routing”, in *Proc. 27th Europ. Symp. on Algor. (ESA 2019), Leibniz Int. Proc. in Inform. (LIPIcs)*, Schloss Dagstuhl, 2019, vol. 144, pp. 75:1-75:14, doi: https://doi.org/10.4230/LIPIcs.ESA.2019.75.

[11] P. Czerner, and H. Räcke, “Compact Oblivious Routing in Weighted Graphs”, in *Proc. 28th Ann. Europ. Symp. on Algor. (ESA 2020), Leibniz Int. Proc. in Inform. (LIPIcs)*, Schloss Dagstuhl, 2020, vol. 173, pp. 36:1-36:23, doi: https://doi.org/10.4230/LIPIcs.ESA.2020.36.

[12] D. Rachmawati, H. Tamara, S. Sembiring, and M. Budiman, “RSA public key solving technique by using genetic algorithm”, *Journal of Theoretical and Applied Information Technology*, vol. 98, iss. 15, pp. 2990-2999, 2020.

[13] A.K.S. Sabonchi, and B. Akay, “Cryptanalysis of polyalphabetic cipher using differential evolution algorithm”, *Tehnički vjesnik*, iss. 27 (4), pp. 1101-1107, 2020, doi: https://doi.org/10.17559/TV-20190314095054.

[14] B. Akay, “A binomial crossover based artificial bee colony algorithm for cryptanalysis of polyalphabetic cipher”, *Tehnički vjesnik*, iss. 27 (6). pp. 1825-1835, 2020, doi: https://doi.org/10.17559/TV-20190422225110.

[15] A.K.S. Sabonchi, B. Akay, “A survey on the Metaheuristics for Cryptanalysis of Substitution and Transposition Ciphers”, *Computer Systems Science And Engineering*, vol. 39, no. 1, pp. 87-106, 2021, doi: http://doi.org/10.32604/csse.2021.05365.

[16] H. Grari, S. Lamzabi, A. Azouaoui, and K. Zine-Dine, “Cryptanalysis of Merkle-Hellman cipher using ant colony optimization”, *Int. Jour. Artif. Intell. (IJ-AI)*, vol. 10, no. 2, pp. 490-500, 2021, doi: https://doi.org/10.11591/ijai.v10.i2.

[17] K. Dworak, and U. Boryczka, “Breaking Data Encryption Standard with a Reduced Number of Rounds Using Metaheuristics Differential Cryptanalysis”, *Entropy*. vol. 23, iss. 12, pp. 1697-1718, 2021, doi: https://doi.org/10.3390/e23121697.

[18] O.O. Kubaychuk, “Osoblyvosti zastosuvannia alhorytmu ASO do deiakykh zadach kryptoanalizu”, *Naukoiemni tekhnolohii*, no. 2 (58), pp. 141-148, 2023, doi: https://doi.org/10.18372/2310-5461.58.17650

[19] O.O. Kubaychuk, “Ohliad zastosuvannia metaevrystychnoho pidkhodu v kryptoanalizi”, *Visnyk KhNTU: informatsiini tekhnolohii*, no. 2 (85), pp. 147-153, 2023, doi: https://doi.org/10.35546/kntu2078-4481.2023.2.20

[20] R. Motwani, and P. Raghavan, *Randomized Algorithms*. Cambridge, GB: Cambridge Univ. Press, 1995.

[21] M. Mitzenmacher, and E.Upfal, *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. Cambridge, GB: Cambridge Univ. Press, 2005.

OKSANA KUBAYCHUK,
DENIS SAI

RANDOMIZED ALGORITHMS IN SYSTEMS WITHOUT COORDINATION AND CENTRALIZATION

Evaluating the complexity of algorithms based only on the possibility of the worst possible variant of the input data is often not justified. The development of algorithms that would predictably work quickly on all possible inputs is of practical importance. If for the problem there is a reasonable opportunity to model the distributions of input values, then you can use probabilistic analysis as a method of developing effective algorithms. When the information about the distribution of input values is not enough for their numerical modeling, algorithms are developed by giving a part of the algorithm itself a random character - randomized algorithms.

The use of randomization ensures the operation of the algorithm with minimal needs to store internal states and events in the past, and the algorithms themselves look compact.

The paper studies problems for which there are relatively effective deterministic algorithms for solving. But, as will be shown, the construction of appropriate randomized algorithms leads to effective and efficient parallel computing schemes with linear complexity on average. The advantages of randomization are especially evident in the case of large computer systems and communication networks that function without coordination and centralization. Examples of such distributed systems are, in particular, networks of currently popular cryptocurrencies. The use of randomized heuristics allows the system to adapt to changing operating conditions and minimizes the likelihood of conflicts between processes.

The paper shows the advantages of using a randomized algorithm over deterministic algorithms for the problem of routing in a network with a hypercube topology. A theorem on estimating the expected number of steps required by Valiant's randomized algorithm to deliver all messages to an address is proved. The expected linear complexity of Valiant's algorithm is a direct consequence of the proven theorem.

Keywords: randomized algorithm, parallel computing, probabilistic analysis, average complexity, Chernov-Heffding inequalities, Markov inequality, hypercube routing.

Кубайчук Оксана Олексіївна, кандидат фізико-математичних наук, доцент, доцент кафедри кібербезпеки та захисту інформації, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-5135-3688, o.kubaychuk@gmail.com.

Сай Денис Максимович, курсант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0009-0009-0185-0991, denissaj@gmail.com.

Kubaychuk Oksana, candidate of sciences in mathematics, associate professor at the cybersecurity and information security academic department, Institute of special communications and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Sai Denis, cadet, Institute of special communications and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.