Конференція молодих вчених 2023
XLI НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ
МОЛОДИХ ВЧЕНИХ ТА СПЕЦІАЛІСТІВ
ІНСТИТУТУ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ
ІМ. Г.Є. ПУХОВА НАН УКРАЇНИ
17 травня 2023 р.,
м. Київ, Україна

ДОСЛІДЖЕННЯ МЕТОДУ ВЕРИФІКАЦІЇ TLC ПРИ ВИРІШЕННІ ЗАДАЧ ЕНЕРГЕТИКИ

В.В. Шкарупило, І.В. Блінов, В.В. Душеба

Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України,
Інститут електродинаміки НАН України

Актуальність

- Адресується проблема зростання простору станів системи переходів, що будується при вирішенні задачі формальної верифікації методом перевірки на моделі, – з точки зору відповідних обчислювальних і просторових витрат.
- Названу проблему опрацьовано шляхом дослідження реалізацій поширеного формального методу перевірки на моделі TLC (TLA Checker; by L. Lamport). Досліджено дві альтернативні реалізації методу TLC – з точки зору супутніх обчислювальних і просторових витрат: BFS (Breadth-first Search) – застосовується за замовчанням; альтернативна реалізація DFS (Depth-first Search) [3-7].
- Ідея полягає в тому, щоб оцінити та порівняти альтернативні реалізації методу TLC, ґрунтуючись на заданому сценарії предметної області – з позиції супутніх обчислювальних і просторових витрат, які мають місце під час перевірки на моделі. Цей підхід є спробою виявити та оцінити фактори – наприклад, архітектуру (структуру та зв’язки), подану у формальній специфікації, кількість змінних станів тощо – що впливають на обчислювальні та просторові витрати, супутні застосуванню заданої реалізації методу формальної верифікації (у нашому випадку – TLC). Більше того, було також здійснене намагання оцінити результат впровадження багатопоточності в реалізації методу TLC.

Огляд літератури

- На сьогоднішній день рівень деталізації при перевірці несуперечності сучасних програмно-алгоритмічних рішень, що стосуються сценаріїв, що відбуваються у різних сферах, критичних до безпечності, наприклад, сценарії енергетики (атомна промисловість Фінляндії), авіоніка (сценарії управління режимом роботи супутника), програмна система керування рухом залізничного транспорту тощо, як правило, обмежується, у тому числі, обчислювальними і просторовими ресурсами, необхідними для успішного застосування перевірених часом формальних методів верифікації та супутніх засобів – через експоненційне зростання простору станів системи переходів, що будується і обходиться при автоматизованій формальній верифікації методом перевірки на моделі.
- Наприклад, адресуючи, зокрема, предметну область авіоніки, результати попередніх проведених досладжень показали зростання як просторових, так і обчислювальних витрат на здійснення формальної верифікації, із зростанням числа змінних станів [3, 4].
- Дієвий підхід до зниження зазначеного вище ефекту – варіювання рівня атомарності формальної специфікації, оперуючи групами властивостей – «гіпервластивостями», із залученням широко застосовуваної темпоральної логіки дій TLA (автор – Леслі Лемпорт) і відповідного методу перевірки на моделі TLC.
- Альтернативний підхід – підхід, заснований на декомпозиції: формальна специфікація розкладається на підспецифікації, які потім перевіряються за допомогою перевіреного часом методу Event-B (K. Kraibi та ін.).

Огляд літератури

- Ще одним перспективним підходом до зменшення обчислювальних витрат залучення засобів mu-числення – для варіювання рівня атомарності формалізованого подання (V. Nardone et al.).
- Крім того, дієвими є застосування підходу «bounded model checking» (H. Gao et al.), залучення засобу Reduced Ordered Binary Decision Diagrams (ROBDDs) (A. Biere et al.).
- Також застосовуються рішення у напрямі комбінуваннядедуктивної верифікації із перевіркою на (J. Amilon et al.).
- У напрямі досягнення компромісу між характеристиками перевірки на моделі (експоненційне зростання простору станів системи переходів) і характеристиками тестування, існують намагання побудувати «міст» між перевіркою на моделі, що застосовується на етапі проєктування процесу розроблення, та валідацією шляхом тестування – інструментарій MET (Model Checking-driven Explorative Testing) (Y. Zhang et al.).
- Крім того, застосовується підхід до композиційної перевірки на моделі: наприклад, із залученням інструментарію Interaction-Preserving Abstraction (IPA), з використанням формалізму TLA+ (X. Gu et al.).

Деякі результати попередніх досліджень

- Синтетичний сценарій: послідовний сценарій (табл. 1; рис. 1).
- Результати отримано на наступній тестовій платформі: AMD K10, 3,0 ГГц; 2 ГБ ОП стандарту DDR3; операційна система – MS Windows 7; середовище виконання – Java Runtime Environment v. 1.7 (JRE).

Таблиця 1 – Обчислювальні витрати

№ з/п	n	$\lvert S \rvert$	$\bar{t}_{BFS}$, с	$\bar{t}_{DFS}$, с	$\bar{t}_{BFS} / \bar{t}_{DFS}$
1	2	3	4	5	6
1	2^1	5	0,934	0,420	2,224
2	2^2	9	0,952	0,450	2,115
3	2^3	17	1,029	0,540	1,906
4	2^4	33	1,154	0,770	1,499
5	2^5	65	1,412	3,170	0,446
6	2^6	129	2,970	35,750	0,083
7	2^7	257	19,210	-	-
8	2^8	513	-	-	-

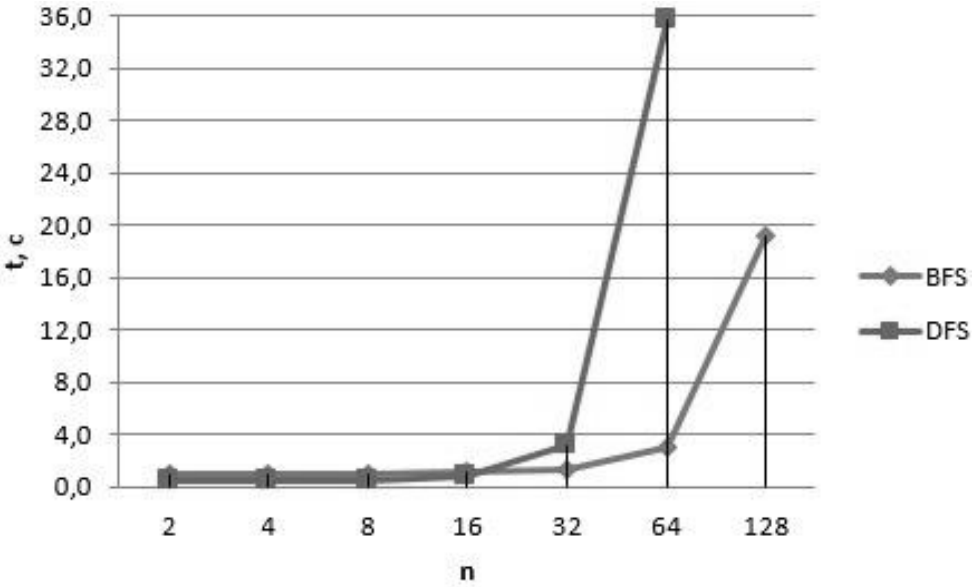

Рисунок 1 – Графік зростання обчислювальних витрат

Деякі результати попередніх досліджень

- Результати отримано на оновленій тестовій платформі: CPU – AMD Ryzen R5 2400g; RAM – 16 GB; Java Runtime Environment, version “1.8.0_241”; TLC version: 2.14 of 10 July 2019.

Таблиця 2 – Доповнення результатів табл. 1

№ з/п	n	$\lvert S \rvert$	$\bar{t}_{BFS}$, с	$\bar{t}_{DFS}$, с	$\bar{t}_{BFS} / \bar{t}_{DFS}$
1	2	3	4	5	6
1	2^1	5	0,880	0,310	2,839
2	2^2	9	0,890	0,390	2,282
3	2^3	17	0,930	0,460	2,022
4	2^4	33	1,070	0,670	1,597
5	2^5	65	1,430	1,620	0,883
6	2^6	129	2,160	17,390	0,124
7	2^7	257	6,390	226,970	0,028
8	2^8	513	38,980	3687,330	0,011

Деякі результати попередніх досліджень

- Результати оцінювання супутніх просторових витрат.

Таблиця 3 – Доповнення результатів табл. 1

№ з/п	n	$\lvert S \rvert$	$\lvert S^*_{BFS} \rvert$	$\lvert S^*_{DFS} \rvert$	$\frac{\lvert S \rvert}{\lvert S^*_{BFS} \rvert}$	$\frac{\lvert S \rvert}{\lvert S^*_{DFS} \rvert}$	$\frac{\lvert S^*_{DFS} \rvert}{\lvert S^*_{BFS} \rvert}$	b , байтів
1	2	3	4	5	6	7	8	9
1	2^1	5	21	41	0,238	0,122	1,952	681
2	2^2	9	73	289	0,123	0,031	3,959	1331
3	2^3	17	273	2177	0,062	0,008	7,974	3293
4	2^4	33	1057	16897	0,031	0,002	15,986	10230
5	2^5	65	4161	133121	0,016	$4{,}88 \cdot 10^{-4}$	31,993	35702
6	2^6	129	16513	1056769	0,008	$1{,}22 \cdot 10^{-4}$	63,996	132896
7	2^7	257	65793	8421377	0,004	$3{,}05 \cdot 10^{-5}$	127,998	527085
8	2^8	513	262657	67239937	0,002	$0{,}76 \cdot 10^{-5}$	255,999	2169856

Деякі результати попередніх досліджень

- Сценарій предметної області із галузі авіоніки.

Таблиця 4 – Показники обчислювальної складності

№ з/п	n	$\bar{t}_{BFS}$, с	$\bar{t}_{DFS}$, с	$\bar{t}_{DFS}/\bar{t}_{BFS}$	$depth$, вершин
1	2	3	4	6	7
1	4	0,893	0,437	0,489	10
2	6	0,929	0,477	0,513	15
3	7	0,957	0,554	0,579	18
4	7	0,969	0,578	0,596	19
5	8	1,001	0,788	0,787	22
6	10	1,140	1,505	1,320	27
7	11	1,448	2,577	1,780	30
8	11	1,468	2,674	1,822	31
9	12	1,682	4,818	2,864	34
10	14	2,460	19,751	8,029	39
11	15	3,552	44,575	12,549	42
12	15	3,560	53,226	14,951	43
13	16	5,370	105,340	19,616	46
14	17	9,666	273,970	28,344	49
15	18	17,127	581,860	33,973	52

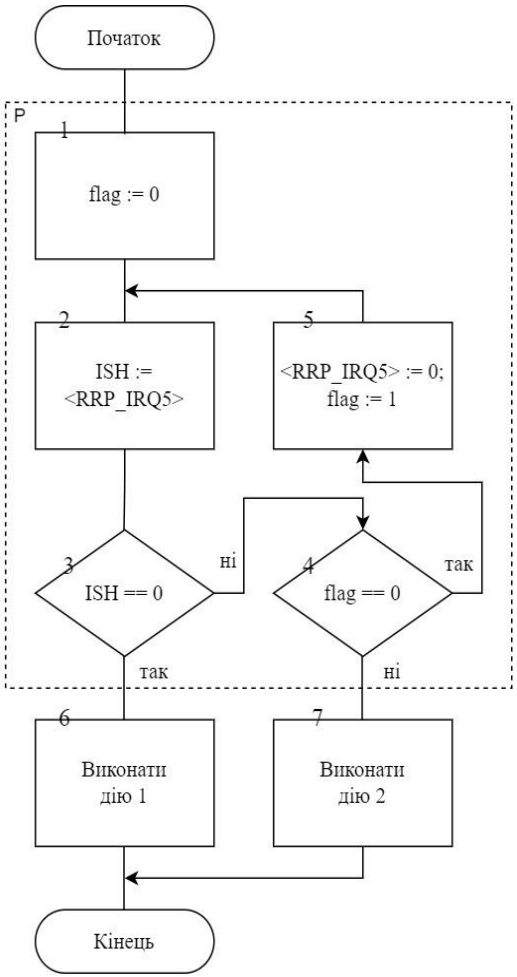

Рисунок 2 – Фрагмент блок-схеми алгоритму

Деякі результати попередніх досліджень

- Сценарій предметної області із галузі авіоніки.

Таблиця 5 – Показники просторової складності

№ з/п	n	$\lvert S \rvert$	$\lvert S^*_{BFS} \rvert$	$\lvert S^*_{DFS} \rvert$	$\frac{\lvert S \rvert}{\lvert S^*_{BFS} \rvert}$	$\frac{\lvert S \rvert}{\lvert S^*_{DFS} \rvert}$	$\frac{\lvert S^*_{DFS} \rvert}{\lvert S^*_{BFS} \rvert}$	$depth$, вершин
1	2	3	4	5	6	7	8	9
1	4	82	130	700	0,631	0,117	5,385	10
2	6	342	534	4519	0,640	0,076	8,463	15
3	7	702	1086	11189	0,646	0,063	10,303	18
4	7	712	1096	11927	0,650	0,060	10,882	19
5	8	1432	2200	28156	0,651	0,051	12,798	22
6	10	5742	8814	141343	0,651	0,041	16,036	27
7	11	11502	17646	317237	0,652	0,036	17,978	30
8	11	11512	17656	328775	0,652	0,035	18,621	31
9	12	23032	35320	726652	0,652	0,032	20,573	34
10	14	92142	141294	3367327	0,652	0,027	23,832	39
11	15	184302	282606	7287605	0,652	0,025	25,787	42
12	15	184312	282616	7471943	0,652	0,025	26,438	43
13	16	368632	565240	16049788	0,652	0,023	28,395	46
14	17	737272	1130488	34311398	0,652	0,021	30,351	49
15	18	1474552	2260984	73046458	0,652	0,020	32,307	52

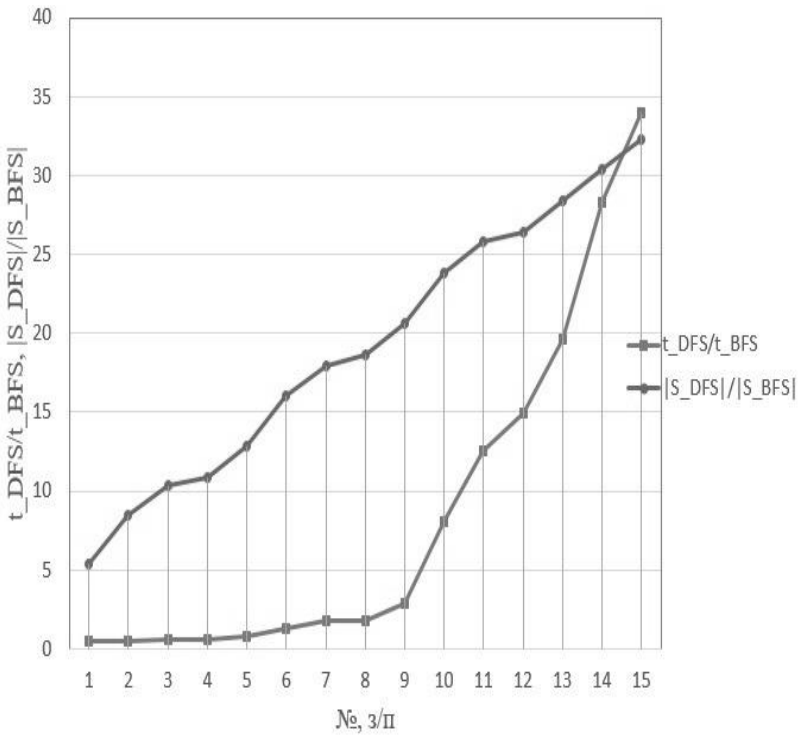

Рисунок 3 – Графік зростання значень відносних показників

Деякі результати попередніх досліджень

- Оцінювання ефекту від введення мультипоточності.

Таблиця 6 – Результати дослідження мультипоточного застосування реалізацій методу

№ з/п	tc	Реалізація методу				$\bar{t}_{DFS} / \bar{t}_{BFS}$
		BFS		DFS		
		$\bar{t}_{BFS}$, с	α	$\bar{t}_{DFS}$, с	α	
1	2	3	4	5	6	7
1	1	3,552	1,000	44,575	1,000	12,549
2	2	3,072	1,156	28,384	1,570	9,240
3	4	2,966	1,198	19,989	2,230	6,739
4	8	2,815	1,262	20,526	2,172	7,292

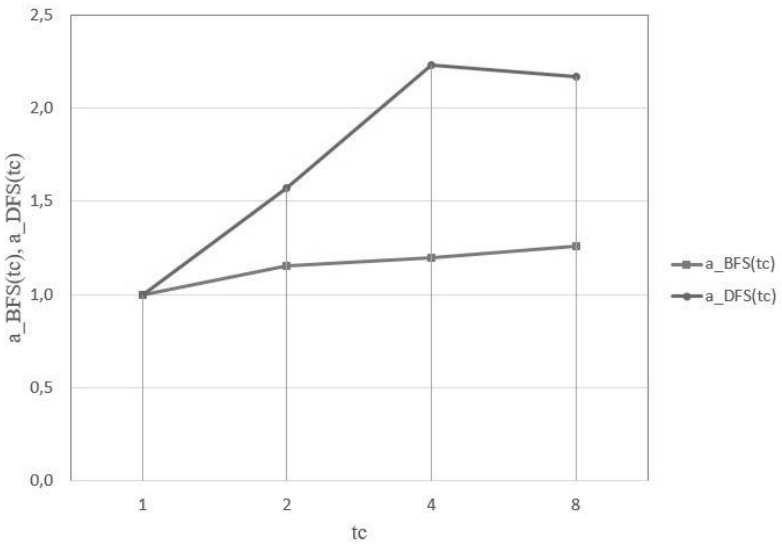

Рисунок 4 – Графік залежності коефіцієнту прискорення від числа програмних потоків

Запропонований і застосований підхід

- У прелставленій праці задачу перевірки на моделі було вирішено на основі сценарію предметної області галузі енергетики – на прикладі артефакту процесу оновлення реєстру європейських ідентифікаційних кодів (згідно лібералізованої моделі взаємодії ENTSO-E).
- Ідея полягає в тому, щоб оцінити та порівняти різні реалізації методу TLC, ґрунтуючись на предметно орієнтованому сценарії – стосовно супутніх обчислювальних і просторових витрат, що мають місце при перевірці на моделі. Цей підхід є спробою виявити та оцінити фактори – наприклад, архітектуру (структуру та зв’язки), подану у формальній специфікації, кількість змінних станів тощо – що впливають на обчислювальні та просторові витрати на формальну верифікацію заданим методом перевірки на моделі – із акцентом на реалізації методу (у нашому випадку – методу TLC). Крім того, також була зроблена спроба оцінити ефект від введення мультипоточності до реалізації методу TLC.
- Як показову проблемну область, де мають місце різноманітні критичні для безпеки сценарії, розглянуто сучасний ринок електроенергії України, у контексті гармонізованої європейської моделі ринку електроенергії. Процес оновлення реєстру європейських ідентифікаційних кодів було розглянуто як приклад (рис. 5).

Сценарій предметної області

- UML-діаграму, подану на рис. 5, адресовано у якості вихідного артефакту.
- На рис. 5 подано фрагмент рольової моделі процесу оновлення реєстру міжнародних ідентифікаційних кодів (згідно лібералізованої моделі взаємодії ENTSO-E) – UML-діаграма дій. Повна рольова модель охоплює 23 дії, плюс 6 умовних операторів. Названа модель адресується як артефакт – сутність з архітектурою (структурою та зв'язками) та змістом (за М. Броєм) [2].
- Наступний крок – отримати формалізоване подання артефакту, фрагмент якого фігурує на рис. 5. Це виконано згідно підходу, викладеного нижче.

$$|V| = 27, \quad |S| = 290.$$

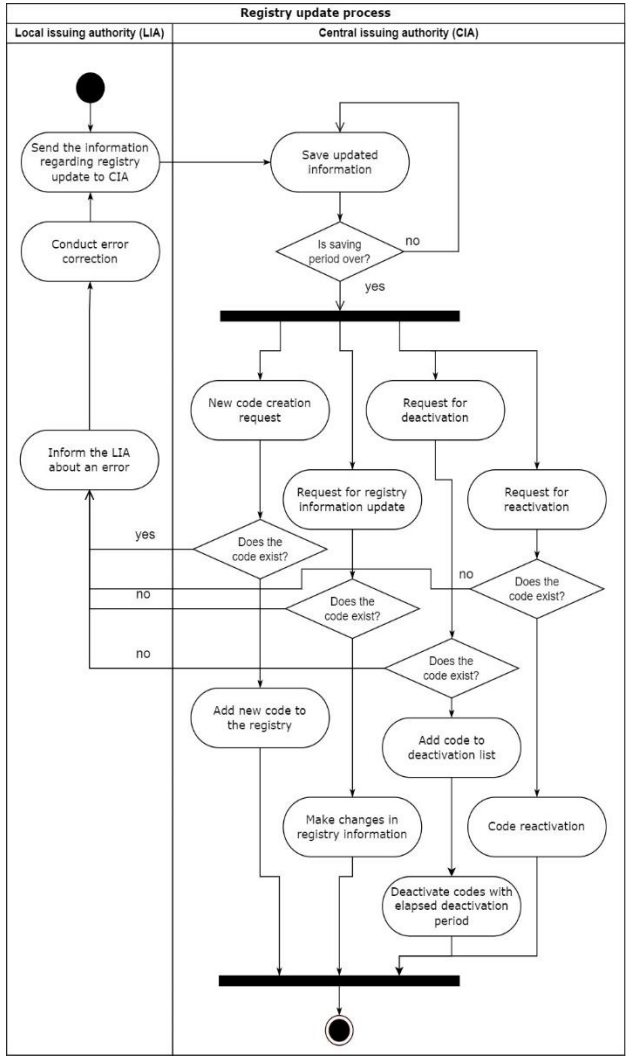

Рисунок 5 – Рольова модель

Застосований підхід

- Щоб отримати формальну специфікацію, придатну для верифікації в автоматизованому режимі, було розроблено і застосовано наступний підхід:
  - Для створення прототипу архітектурної складової цільової специфікації TLA+, яку ще належить синтезувати, була використана алгоритмічна мова PlusCal. Результатом цього кроку є вхідні дані для наступного кроку. Специфікація PlusCal розглядалася як допоміжний артефакт: для подання артефакту рис. 5 у формі PlusCal-подання знадобилося 348 рядків псевдокоду.
  - Для отримання результуючого артефакту – специфікації TLA+ – із псевдокоду PlusCal було використано інструментарій TLA+ Toolbox IDE.
- Специфікацію TLA+ було залучено як вихідну конструкцію для методу перевірки на моделі TLC, призначеного до застосування в автоматизованому режимі. Отримане формалізоване подання містить 508 рядків коду.

Отримані результати

- Конфігурація тестової платформи: CPU – AMD Ryzen R5 2400g; RAM – 16 GB; Java Runtime Environment, version “1.8.0_241”; TLC version: 2.14 of 10 July 2019.

Таблиця 7 – Обчислювальні і просторові витрати, з урахуванням мультипоточності

tn	$f_{BFS}(tn)$, ms	$\alpha_{BFS}(tn)$	$\lvert S^*_{BFS} \rvert$	$f_{DFS}(tn)$, ms	$\alpha_{DFS}(tn)$	$\lvert \overline{S^*_{DFS}} \rvert$	ξ_{DFS}
2^0	1214.000	1.000	336	638.400	1.000	4194.000	1.000
2^1	1157.800	1.049	336	632.900	1.009	5382.890	1.283
2^2	1149.100	1.056	336	665.300	0.960	7267.050	1.733
2^3	1143.800	1.061	336	682.700	0.935	8209.850	1.958

- Із табл. 7 можна побачити, що DFS-реалізація методу TLC виявилася істотно ефективнішою з позиції відповідних обчислювальних витрат, порівняно з альтернативою BFS-реалізацією: від близько 1,902 разів (для $tn = 2^0$) до близько 1,675 разів (для $tn = 2^3$).

Отримані результати

- У намаганні оцінити характер зростання просторових витрат, супутніх застосуванню DFS-реалізації методу TLC (від кількості залучених програмних потоків), було вирішено задачу апроксимації – на основі значень показників tn і ξ_{DFS} (рис. 6). У результаті було отримано наступну оціночну функцію:

$$\xi'_{DFS}(tn)^{-1} = (a + b/tn), \qquad (1)$$

де $a = 0.435$, $b = 0.603$, коефіцієнт детермінації $R^2 = 0.986$.

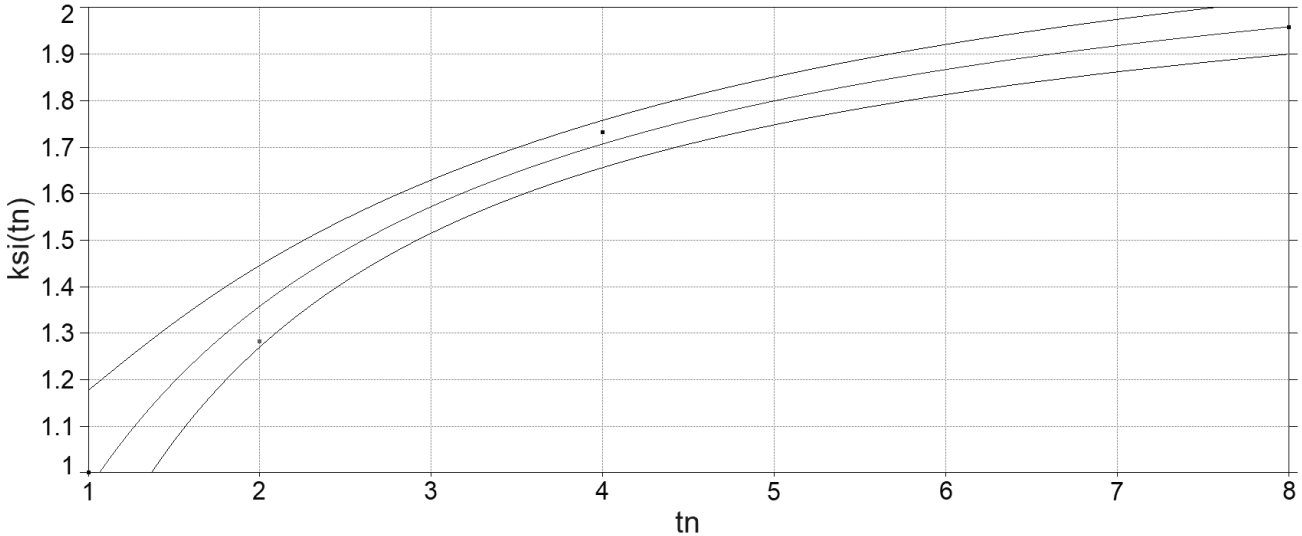

Рисунок 6 – Подання отриманої оцінки характеру зростання просторових витрат

Висновки

- Таким чином, широко застосовуваний метод перевірки на моделі TLC було досліджено у межах представленої праці на основі сценарію предметної області із галузі енергетики. Названий сценарій адресовано у формі відповідних подань – артефактів: подань процесу оновлення реєстру європейських ідентифікаційних кодів. Отримано підтвердження узгодженості відповідної програмно-алгоритмічної складової, із залученням реалізацій методу TLC. Для контролю адекватності результуючого формалізованого подання було застосовано раніше розроблену методику.
- Отримані результати дозволили, зокрема, дійти висновку, що обчислювальні і просторові витрати, супутні застосуванню DFS-реалізації методу TLC, істотно залежить як від кількості змінних стану, які фігурують у формальній специфікації, так і від архітектурної складової останньої. У той же час, загалом, на основі дослідженого сценарію предметної області, реалізація DFS виявилася приблизно в 1,675 – 1,902 рази ефективнішою з точки зору супутніх часових витрат, порівняно з альтернативною BFS-реалізацією методу TLC. У противагу, якщо розглядати просторові аспекти (кількість згенерованих станів системи переходів), реалізація DFS виявилася значно гіршою, порівняно з альтернативною BFS-реалізацією: від приблизно 12,482 до приблизно 24,434 разів.
- Також здійснено спробу оцінити характер зростання просторових витрат, супутніх застосуванню DFS-реалізації методу TLC, в залежності від числа залучених програмних потоків. Для цього було вирішено задачу апроксимації.

Посилання

- [1] Blinov I., Tankevych S. The harmonized role model of electricity market in Ukraine. 2016 2nd International Conference on Intelligent Energy and Power Systems, IEPS (Kyiv, Ukraine, June 07–11, 2016). doi: https://doi.org/10.1109/IEPS.2016.7521861
- [2] Broy M. A logical approach to systems engineering artifacts and traceability: from requirements to functional and architectural views. Engineering dependable software systems: NATO Science for Peace and Security Series - D: Information and Communication Security / eds. M. Broy, D. Peled, G. Kalus. Amsterdam: IOS Press, 2013. Vol. 34. P. 1-48. DOI: https://doi.org/10.3233/978-1-61499-207-3-1
- [3] Shkarupylo V., Blinov I., Chemeris A., Dusheba V., Alsayaydeh J., Oliinyk A. Iterative Approach to TLC Model Checker Application. Proc. 2021 IEEE KhPI Week on Advanced Technology (Kharkiv, Ukraine, September 13 – 17, 2021). P. 283–287. DOI: https://doi.org/10.1109/KhPIWeek53812.2021.9570055
- [4] Shkarupylo V., Alsayaydeh J.A.J, Tomičić I., Chemeris A., Dusheba V. A technique for checking the adequacy of formal model. ARPN Journal of Engineering and Applied Sciences. August 2021. Vol. 16, No. 16. P. 1707-1719. URL: http://www.arpnjournals.org/jeas/research_papers/rp_2021/jeas_0821_8670.pdf (дата звернення: 28.04.2023).
- [5] Shkarupylo V. V., Tomičić I., Kasian K. M. The investigation of TLC model checker properties. Journal of Information and Organizational Sciences. 2016. Vol. 40, No. 1. P. 145-152. DOI: https://doi.org/10.31341/JIOS.40.1.7
- [6] Shkarupylo V. V., Tomičić I., Kasian K. M., Alsayaydeh J. A. J. An Approach to increase the Effectiveness of TLC Verification with Respect to the Concurrent Structure of TLA+ Specification. International Journal of Software Engineering and Computer Systems. 2018. Vol. 4, No. 1. P. 48-60. DOI: https://doi.org/10.15282/ijsecs.4.1.2018.4.0037
- [7] Shkarupylo V., Blinov I., Dusheba V., Alsayaydeh J. A. J. Case Driven TLC Model Checker Analysis in Energy Scenario. Proc. of the Sixth International Workshop on Computer Modeling and Intelligent Systems, CMIS-2023 (Zaporizhzhia, Ukraine, May 3, 2023). P. 65-75. URL 1: https://www.youtube.com/watch?v=MErmrlRdLg0 URL 2: https://ceur-ws.org/Vol-3392/ URL 3: https://ceur-ws.org/Vol-3392/paper6.pdf (дата звернення: 28.04.2023).