УДК 004.056.5

І. Дронюк, М. Назаркевич, В. Тхір
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

ОЦІНКА РЕЗУЛЬТАТІВ МОДЕЛЮВАННЯ ПЕРІОДИЧНИХ *ATEB*-ФУНКЦІЙ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Розроблено методи для знаходження значень періодичних Ateb-функцій. Для числового моделювання застосовано розклади Ateb-функцій у ряди Тейлора та Фур'є. Результати обчислення проілюстровано графіками. Реалізовано порівняльну оцінку обчислень за допомогою розкладів у ряди Тейлора та Фур'є. Розроблені алгоритми пропонується застосувати для захисту інформації.

Ключові слова: програмне забезпечення, Ateb-функції, захист інформації.

Methods are built for finding of values periodic Ateb-functions. For the numerical simulation the schedules of Ateb-functions are applied to the Taylor and Fourier rows. The results of calculation are illustrated by the graphs. Comparative estimation of calculations is realized with series in the Taylor and Fourier rows. It is suggested to apply the developed algorithms for defence of information.

Keywords: software, Ateb-function, defence of information.

Вступ

Захист інформації у друкованому та електронному вигляді є актуальною проблемою. Розвиток комп'ютерної техніки спонукає до постійного оновлення методів та засобів захисту інформації [1]. У цій роботі пропонується застосувати для захисту друкованої та електронної інформації теорію *Ateb*-функцій. З цією метою розроблено методи обчислення значень періодичних *Ateb*-функцій, основаних на розкладах у ряди Тейлора та Фур'є.

Аналітичні вирази для *Ateb*–функцій отримано у роботах [2,3]. Проте аналітичний запис розв'язків не є зручним для числового моделювання за цими формулами. Труднощі обчислень пов'язані з особливістю виразів, які є оберненням інтегралів, що входять у формули розв'язків. Отже розроблені прості та зручні у користуванні алгоритми обчислення періодичних *Ateb*-функцій є актуальними для захисту інформації запропонованим методом.

Моделювання Ateb-функцій за допомогою розкладу в ряд Тейлора

Для розв'язання різноманітних практичних задач необхідно отримати числові значення *Ateb*-функцій. Періодичність *Ateb*-функцій уможливлює розв'язання цієї задачі двома методами: за допомогою розкладу у ряд Тейлора та ряд Фур'є. Оцінку ефективності розроблених методів виконуємо для значень параметрів *Ateb*-функцій $n = m = 1$, що відповідає випадку тотожності *Ateb*-функцій зі звичайними тригонометричними функціями.

Відомо [4], що обчислювати досить тільки одну з *Ateb*-функцій. Будемо обчислювати функцію *Ateb*-синуса $sa(n, m, w)$. За означенням *Ateb*-синуса введемо у розгляд функцію

$$\Phi(w) = w - \frac{n+1}{2}\int_0^w \frac{d\bar{v}}{(1-\bar{v}^{n+1})^{\frac{m}{m+1}}} \qquad (1)$$

У роботі [5] подано формули розкладу *Ateb*-синусу у ряд Тейлора, а у роботі [6] запропоновано метод обчислення значень *Ateb*-синусу за допомогою ряду Тейлора.

Для реалізації обчислень визначених інтегралів використано методи прямокутників, трапецій та парабол [7]. Для перевірки ефективності кожного методу реалізовано обчислення *Ateb*-синуса за значень $n = m = 1$, що відповідає звичайному синусу. Обчислення виконано на проміжку $\left[0, \frac{\Pi}{2}\right]$, де Π – період *Ateb*-синуса, що за цих значень параметрів збігається з числом $p = 3{,}1415926535$.

Існують різні методи обчислення нулів функції: метод золотого перерізу, метод Фібоначі, дихотомічний метод та інші [7]. Для знаходження нулів функції (1) використовується метод поділу відрізку наполовину. З цією метою задається достатньо малий додатний параметр $e\left(e = 10^{-10}\right)$. Процес обчислення продовжується доти, доки s-й відрізок не стане величиною порядку e, тобто

$$|w_{s+1} - w_s| \le e\ , \tag{2}$$

де w_s – наближення на s-му кроці.

Тоді за нуль функції $\Phi(w)$ приймаємо величину

$$w = \frac{1}{2}(w_{s+1} + w_s)\ .$$

Отже, реалізовано обчислення значення *Ateb*-синуса, на основі використання розкладу в ряд Тейлора та методів наближеного обчислення інтеграла та нулів функції. Описаний метод реалізовано у відповідному програмному забезпеченні.

Моделювання Ateb-функцій за допомогою розкладу в ряд Фур'є

Будь-яку періодичну функцію $F(w)$ з періодом $2\Pi = [-\Pi, \Pi]$ можна розкласти на цьому відрізку в ряд Фур'є за формулами

$$F(w) = \frac{a_0}{2} + \sum_{k=1}^{\infty}\left(a_k \cos\frac{kpw}{\Pi} + b_k \sin\frac{kpw}{\Pi}\right) \tag{3}$$

Оскільки функція *Ateb*-синуса $sa(n, m, w)$ є непарною, то в розкладі (3) коефіцієнти $a_k = 0$, (k=0,…,∞). У результаті розклад в ряд Фур'є для *Ateb*-синуса має вигляд

$$sa(n, m, w) = \sum_{k=1}^{\infty} b_k \sin\frac{kpw}{\Pi} \tag{4}$$

де

$$b_k = \frac{1}{\Pi}\int_{-\Pi}^{\Pi} sa(n, m, y)\sin\frac{kpy}{\Pi}\,dy = \frac{n+1}{2\Pi}\int_{-\Pi}^{\Pi}\sin\frac{kpy}{\Pi}\int_{0}^{-1\le y\le 1}\frac{d\bar{y}}{\left(1-\bar{y}^{n+1}\right)^{\frac{m}{m+1}}}dy\ . \tag{5}$$

У [8] доведено, що ряди (4) є збіжним.

Використаємо формулу (4) для обчислення *Ateb*-синуса. Основна складність обчислення полягає у розрахунку коефіцієнтів розкладу в ряд Фур'є, заданих формулами (5). Як видно з виведених формул, b_k подано у вигляді подвійних інтегралів. У записаному представленні внутрішній інтеграл є невластивим, адже при $y \to 1$ для b_k підінтегральні вирази прямують до нескінченності.

Опишемо метод обчислення *Ateb*-функцій за допомогою розкладів у ряди Фур'є. На початковому етапі вводимо вхідні дані: крок ітерації та параметри *Ateb*-функцій n і m. Після введення параметрів n і m перевіряємо умову періодичності. Після цього обчислюємо період *Ateb*-функції $\Pi(m, n)$. Обчислення виконуємо на проміжку $\left[0, \frac{1}{2}\Pi(m, n)\right]$ з певним заданим кроком. Далі обчислюємо функцію *Ateb*-синуса згідно з (4) за допомогою ряду Фур'є. Обчислюємо суму ряду до заданої точності.

Обчислені значення функції виводимо у файл або на дисплей та зберігаємо у масив з метою побудови графіків функції, після чого вибираємо наступну точку. Якщо ця точка належить проміжку, то повертаємось до обчислень, якщо функція обчислена на всьому проміжку, то виводимо результати обчислень. Окремим блоком виділимо обчислення коефіцієнтів b_k, (k=1,…,∞), що є невластивими інтегралами. Для їх обчислення використано наближені методи обчислення подвійних інтегралів та дихотомічний метод пошуку нулів функції [7].

У такий спосіб реалізовано метод обчислення періодичних *Ateb*-функцій на основі розкладу у ряди Фур'є та методів наближених обчислень. Відповідно до описаного методу розроблено комп'ютерну програму.

Порівняння методів моделювання Ateb-синуса рядами Тейлора та Фур'є

Для реалізації описаних методів виконано обчислення *Ateb*-синуса при різних значеннях параметрів n і m. На основі розроблених методів реалізовано комп'ютерну програму, інтерфейс якої наведений на рис. 1. Програма виконує обчислення періоду $\Pi(m,n)$ та значень *Ateb*-синуса із заданим кроком на проміжку $[-\Pi(m,n);\Pi(m,n)]$ за двома методами, використовуючи ряди Тейлора та Фурє. Обчислені значення виводяться на екран та у файл. На їх основі будуються графіки *Ateb*-синуса та виводяться на екран. На рис. 1 наведено приклад роботи програми для значення $m=1, n=\frac{1}{3}$.

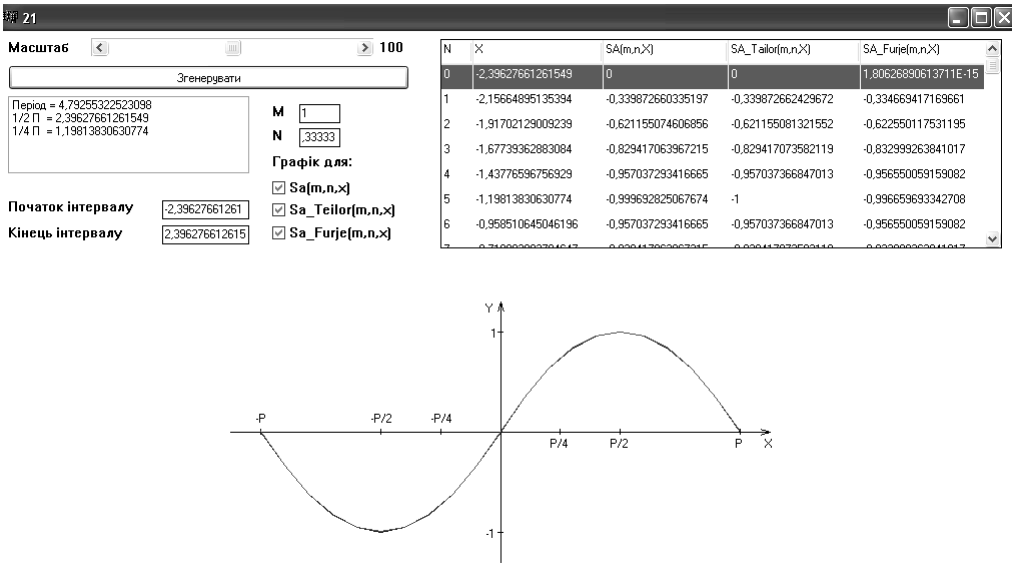
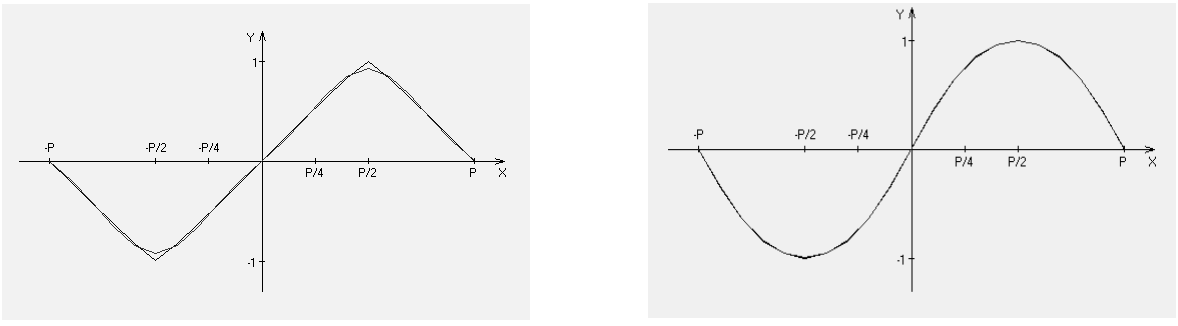


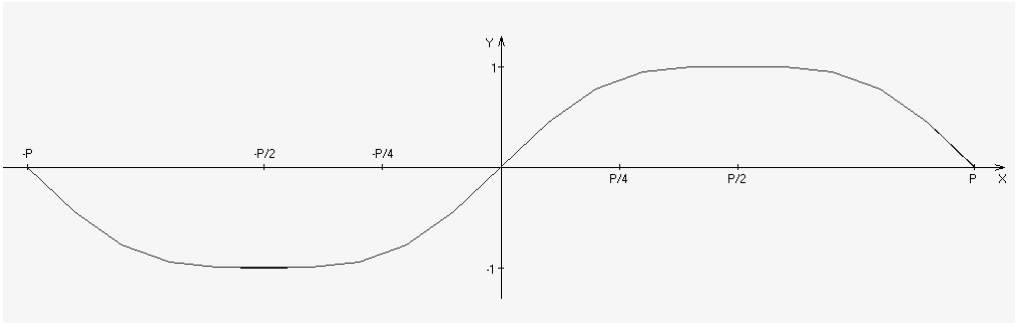
Рис. 1. Інтерфейс комп'ютерної програми



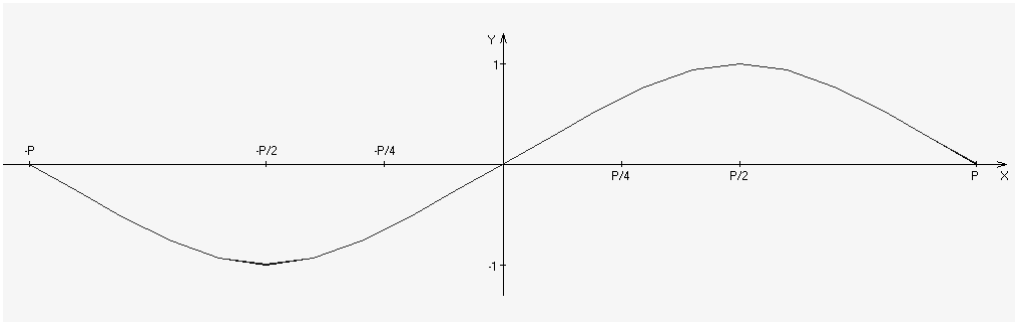
а *б*

Рис. 2. Графік Ateb-синуса для а) $m=1, n=\frac{1}{3}$ *; б)* $n=1, m=\frac{1}{3}$ *період* $\Pi = 4{,}7925532252$

На рис. 2 наведено відповідні графіки *Ateb*-синуса для значень параметрів $m=1, n=\frac{1}{3}$ та $n=1, m=\frac{1}{3}$. Обчислення виконано на основі двох методів, основаних на розкладах у ряди Тейлора та Фур'є. На рис. 3 показано графіки *Ateb*-синуса для значень параметрів $m=1; n=2{,}5$ та $m=2{,}5; n=1$. Як видно на рис. 2, 3, побудовані за обома методами графіки збігаються, оскільки розраховані значення відрізняються цифрами після 10^{-6} порядку. Для визначення ефективності обчислень за допомогою кожного з цих методів виконано порівняння результатів моделювання.



а



б

Рис. 3. Графік Ateb-синуса для
а) $m=1; n=2{,}5$ *; б)* $m=2{,}5; n=1$ *період* $\Pi = 9{,}4550717143$

Оцінка результатів моделювання Ateb-синуса

Виконаємо порівняльний аналіз результатів моделювання *Ateb*-функцій. Для реалізації порівняння вибираємо обчислення за рядами Тейлора та Фур'є *Ateb*-синуса для значень параметрів $n=m=1$, що відповідає випадку тотожності *Ateb*-функції зі звичайним тригонометричним синусом. Значення звичайного синуса вибрано за точні у формулах розрахунку похибки обчислень. У таблиці наведено результати обчислень значень *Ateb*-синуса $sa(1,1,w)$ на проміжку $\left[0,\frac{1}{2}\Pi(1,1)\right]$ з кроком $\frac{1}{20}\Pi(1,1)$ за допомогою рядів Тейлора і Фур'є та методів наближених обчислень, а також відповідні відносні похибки обчислень.

На рис. 4 наведено графіки відносних похибок обчислень значень *Ateb*-синуса sa(1,1,ω) на проміжку $\left[0,\frac{1}{2}\Pi(1,1)\right]$ з кроком $\frac{1}{20}\Pi(1,1)$ за допомогою рядів Тейлора і Фур'є. З показаних графіків випливає, що похибка обчислень за допомогою ряду Тейлора зростає з наближенням до точок екстремуму $\pm\frac{\Pi}{2}$, а похибка обчислень з використанням ряду Фур'є зменшується з наближенням до точок перегину $\pm\frac{\Pi}{4}$. Проте порядок максимальної відносної похибки обчислень у обох випадках

дорівнює 10^{-3}, що свідчить про високу ефективність обох запропонованих методів. Отже, для практичного використання у випадку періодичних *Ateb*-функцій рекомендується використовувати моделювання як на основі рядів Тейлора, так і на основі рядів Фур'є.

Оцінка результатів моделювання Ateb-синуса з використанням ряду Тейлора та ряду Фур'є

i Ітерація,	ω_i	Синус $\sin(\omega_i)$	$sa(1,1,\omega_i)$, за ряд	$sa(1,1,\omega_i)$, за р	ибка за рядом	Відносна похибка за рядом Фур'є, (%)
1	0,0785398163	0,0784590957	0,0784590957	0,0784626165	0,0000000000	0,0044874224
2	0,1570736327	0,1564344650	0,1564344650	0,1564412237	0,0000000030	0,0043204134
3	0,2356194490	0,2334453639	0,2334453639	0,2334548105	0,0000000021	0,0040466298
4	0,3141592654	0,3090169944	0,3090169944	0,3090283440	0,0000000017	0,0036728181
5	0,3926990817	0,3826834324	0,3826834324	0,3826957095	0,0000000014	0,0032081828
6	0,4712386980	0,4539904997	0,4539904997	0,4540025948	0,0000000014	0,0026641649
7	0,5497787144	0,5224985647	0,5224985647	0,5225092977	0,0000000016	0,0020541599
8	0,6283185307	0,5877852523	0,5877852523	0,5877934412	0,0000000005	0,0013931870
9	0,7068583471	0,6494480483	0,6494480483	0,6494525784	0,0000000043	0,0006975270
10	0,7353981634	0,7071067811	0,7071067812	0,7071066702	0,0000000089	0,0000156941
11	0,8539379797	0,7604059655	0,7604059656	0,7604004228	0,0000000198	0,0007289089
12	0,9424777961	0,8090169940	0,8090169944	0,8090054692	0,0000000470	0,0014245454
13	1,0210176124	0,8526401633	0,8526401644	0,8526223820	0,0000001207	0,0020854438
14	1,0995574288	0,8910065211	0,8910065242	0,8909825065	0,0000003432	0,0026952266
15	1,1780972451	0,9238795221	0,9238795325	0,9238496026	0,0000011299	0,0032384581
16	1,2566370614	0,9510564723	0,9510565163	0,9510212870	0,0000046263	0,0036995971
17	1,3351766778	0,9723696611	0,9723699204	0,9723302668	0,0000266660	0,0040513701
18	1,4137166941	0,9876857046	0,9876883406	0,9876453582	0,0002668909	0,0040849393
19	1,4922565105	0,9968616740	0,9969073337	0,9969029228	0,0045803458	0,0041378685

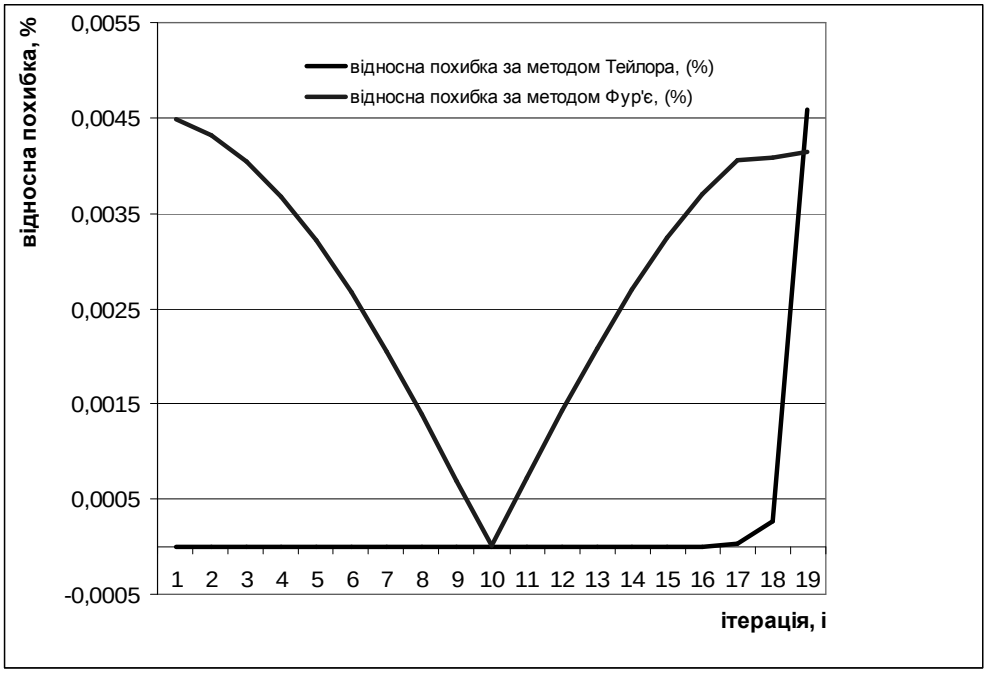


Рис. 4. Відносна похибка обчислень Ateb-синуса за методом Тейлора та Фур'є

Висновки

Для деяких практичних задач захисту інформації пропонується використовувати періодичні *Ateb*-функції. З цією метою розроблено методи моделювання *Ateb*-функцій залежно від параметрів на основі рядів Тейлора і Фур'є. Під час моделювання використовуються методи наближених обчислень інтервалів. Реалізовано порівняння обчислень інтегралів для *Ateb*-функцій на основі різних методів. Наведено методи обчислень *Ateb*-функцій на основі рядів Тейлора і Фур'є. На цій основі розроблено відповідне програмне забезпечення. Подано інтерфейс ужитку, приклади роботи програми проілюстровано за допомогою графіків. Внаслідок порівняння моделювання періодичних *Ateb*-функцій на основі рядів Тейлора і Фур'є зроблено висновок, що обидва методи є ефективними. Здійснено оцінку похибки обчислень за обома методами, згідно з якою відносна похибка обчислень – близько 10^{-3} для обох випадків.

1. Коншин А.А. Защита полиграфической продукции от фальсификации. – Г.: Синус, 1999. – 160 с. 2. Возний А.М. Застосування Ateb-функцій для побудови розв'язків одного класу суттєво нелінійних диференціальних рівнянь // Доповіді АН УССР. Сер. А, 1970. – № 9. – С. 971–974. 3. Сокіл Б.І. Асимптотичні наближення розв'язків для одного нелінійного неавтономного рівняння // Укр. мат. журнал. — 1997. 49, № 11. — С. 1580–1583. 4. Сеник П.М., Возний А.М. Про табулювання періодичної Ateb-функції. Доповіді АН УССР. Сер. А, 1969, № 12, С. 1089–1092. 5. Грыцык В.В., Дронюк И.М., Назаркевич М.А. Информационные технологии защиты документов средствами Ateb-функций // Часть 1. Построение базы данных Ateb-функций для защиты документов // Проблемы управления и автоматики. – 2009. – № 2. – С. 139–152. 6. Грицик В.В., Назаркевич М.А. Математичні моделі алгоритмів і реалізація Ateb-функцій // Доповіді НАН України, Сер. А, 2007, № 12. С. 37 – 437. 7. Цегелик Г.Г. Чисельні методи. – Львів: Вид. ЛНУ ім. І.Франка, 2004. – 408 с. 8. Фихтенгольц Г. М. Курс дифференциального и интегрального исчисления. В 3 т. Т. 3. – 8-е изд. – М.: Физматлит, 2003. – 680 с.