Кібернетика та комп'ютерні технології

УДК 519.6; 519.64 DOI:10.34229/2707-451X.24.2.5

В.К. ЗАДІРАКА, І.В. ШВІДЧЕНКО

МЕТОДИ БОРОТЬБИ З НАКОПИЧЕННЯМ ПОХИБКИ ЗАОКРУГЛЕННЯ ПІД ЧАС РОЗВ'ЯЗАННЯ ЗАДАЧ ТРАНСОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ

Показано, як, використовуючи оцінки похибок заокруглення, будувати стійкі до похибок заокруглення обчислювальні алгоритми. При цьому враховуються: правило заокруглення, режим обчислення, якість оцінок похибок заокруглення (непокращувальна оцінка, асимптотична оцінка, ймовірнісна оцінка). За наявності обчислювальних ресурсів доцільно використовувати асимптотичні оцінки та ймовірнісні як більш точні у порівнянні з мажорантними оцінками.

Ключові слова: *похибка заокруглення, комп'ютерна технологія, дискретне перетворення Фур'є, інтегрування швидкоосцилюючих функцій, інформаційна безпека.*

Вступ. Складність задач, що треба розв'язувати постійно зростає. Найбільша увага нині приділяється розв'язанню задач трансобчислювальної складності. Серед таких задач можна виділити задачі обчислення систем лінійних алгебраїчних рівнянь з кількістю невідомих у декілька десятків мільйонів, цифрової обробки сигналів, розрахунку ядерних реакторів, моделювання фізичних і хімічних процесів, аеродинаміки, захисту інформації тощо.

Неврахування похибки заокруглення під час їх розв'язання призводить до того, що іноді отримуються комп'ютерні рішення, які не відповідають фізичному змісту задачі.

В роботі показано, як можна використати оцінки похибок заокруглення для побудови стійких до похибок заокруглення обчислювальних алгоритмів.

Наведено оцінки похибок заокруглення розв'язання деяких класів задач: дискретного перетворення Фур'є, цифрової обробки сигналів, інтегрування швидкоосцилюючих функцій, комп'ютерної стеганографії, багаторозрядного множення.

Застосування оцінок похибок заокруглення продемонстровано на деяких комп'ютерних технологіях розв'язання перелічених класів задач.

1. ε -розв'язок задачі (наближений розв'язок задачі з точністю $\varepsilon(\varepsilon > 0)$) [1].

Зазвичай, постановка задачі для обчислювальної математики полягає в отриманні ε -розв'язку задачі при заданих обчислювальних ресурсах.

Вважається, що вихідна інформація про задачу задана наближено і при реалізації алгоритму на комп'ютері використовується режим плаваючої коми з τ розрядами у мантис чисел.

Таким чином на ε впливають [2]:

– неусувна похибка $\varepsilon_н$ (за рахунок неточності вхідної інформації, яка є джерелом виникнення так званих некоректно поставлених задач);

– похибка методу $\varepsilon_м$ (за рахунок заміни функції апроксимантом, похідних – скінченними різницями, інтегралів – інтегральними сумами тощо);
– похибка заокруглення $\varepsilon_з$ (виникає за рахунок заміни арифметичних операцій відповідними операціями з заокругленням для забезпечення замкненості системи числення).

В роботі основну увагу приділимо $\varepsilon_з$, тому що при розв'язанні задач трансобчислювальної складності $\varepsilon_з$ може вносити домінуючий вклад в ε.

Тобто для отримання ε-розв'язку задачі має виконуватись співвідношення

$$\rho(\varepsilon) \le \rho(\varepsilon_н) + \rho(\varepsilon_м) + \rho(\varepsilon_з), \tag{1}$$

де $\rho(\cdot)$ – деяка міра похибки наближеного розв'язку задачі.

Умову (1) можна замінити умовами:

$$\rho(\varepsilon_н) \le \delta_н, \rho(\varepsilon_м) \le \delta_м, \rho(\varepsilon_з) \le \delta_з, \tag{2}$$

де $\delta_i \le \alpha_i \cdot \varepsilon,\ \sum_i a_i = 1,\ \alpha_i \ge 0,\ i = н, м, з$.

Якщо під час розв'язання задач малої і середньої складності вважалось, що $\rho(\varepsilon_з) \ll \rho(\varepsilon_н) + \rho(\varepsilon_м)$ і похибкою заокруглення часто нехтували, то під час розв'язання задач трансобчислювальної складності ситуація в корені інша. $\rho(\varepsilon_з)$ стає домінуючою серед $\varepsilon_н$ та $\varepsilon_м$ і треба параметри алгоритму обирати такими, щоб задовільнити умови (1), (2).

Справа у тому, що велика кількість операцій і недосконале правило заокруглення (відсічення) призводить до стрімкого накопичення похибки заокруглення і стає проблематичним задовольнити умови (1), (2).

Треба створювати деякі запобіжники стрімкому зростанню оцінки похибки заокруглення. Один з чинників, який дозволяє це зробити – є використання s-слівної арифметики [3]. В цьому випадку оцінка похибки заокруглення буде пропорційна $2^{-s\cdot\tau}$ і завдяки параметру s можна зменшувати вплив похибки заокруглення на точність наближеного розв'язку задачі і на виконання умов (1), (2).

Параметр s (за умови правильного його вибору) по суті зводить нерозв'язувальну задачу (при невиконанні умов (1), (2)) до розв'язувальної.

s-слівна арифметика попри її використання під час розв'язання задач трансобчислювальної складності щільно використовується при обчисленні основних криптопримітивів у двоключовій криптографії (шифрування, розшифрування інформації, електронний цифровий підпис, його верифікація, криптографічні протоколи тощо).

Треба зазначити, що, як правило, $\varepsilon_н$, $\varepsilon_м$, $\varepsilon_з$ невідомі, але можна знайти їх оцінки $\tilde{\varepsilon}_н$, $\tilde{\varepsilon}_м$, $\tilde{\varepsilon}_з$. При цьому важлива якість цих оцінок. Їх завищеність може призвести до великих обчислювальних ресурсів, необхідних для обчислення ε-розв'язку. Тому особливо цінуються досяжні оцінки похибок, імовірнісні і асимптотичні оцінки [2], а також використання інших правил заокруглення (наприклад, рандомізоване правило заокруглення [4, 5]).

В подальшому розглянемо оцінки похибок заокруглення під час розв'язання деяких важливих класів задач обчислювальної та прикладної математики і їх використання у сучасних комп'ютерних технологіях.

2. Обчислення інтегралів від швидкоосцилюючих функцій

Розглянемо обчислення інтегралу вигляду

$$R(f) = \int_\Omega f(X)\, g(X)\, dX, \tag{3}$$

де Ω – деяка стандартна множина, наприклад, $\Omega \equiv \pi_n : -1 \le x_i \le 1$, $i = \overline{1,n}$, $X = (x_1,...,x_n)$, причому відомий клас функцій F, $f(X) \in F$, $g(X)$ – деяка фіксована швидкоосцилююча функція і є можливість обчислювати N значень функціоналів $L_1(f),...,L_N(f)$, де $L_\nu(f) \in \boldsymbol{L}$, $\nu = \overline{1,N}$, $\boldsymbol{L}$ – задана множина функціоналів. Характерними прикладами таких значень функціоналів можуть бути значення функцій та її похідних у сітці вузлів, на лінії, або на площині, коефіцієнти розкладу функцій у ряди за даними системами базисних функцій [4] тощо.

Інтеграли (3) мають широке коло застосувань, зокрема, для розв'язання багатьох задач цифрової обробки сигналів та зображень, прикладної статистики, моделювання оптичних систем та синтезованих голограм, аналізу і синтезу мовних сигналів, математичного моделювання, інформаційної безпеки тощо.

Розглядаються наступні осцилюючі функції: $e^{-i\omega x}$, $e^{i\omega g(x)}$, $\sin \omega x$, $\cos \omega x$, вейвлет-функція $\psi(x)$ з компактним носієм, $J_m(\omega x)$ – функції Бесселя першого роду порядку m.

Для всіх перелічених осцилюючих функцій побудовані оптимальні за точністю квадратурні та кубатурні формули для різних класів F, F_N, $F_{N,\varepsilon}$ [4, 5], де F_N – звуження класу F на конкретну задачу (занурення $f(x)$ у більш вузький клас, використовуючи той факт, що нам відомі для конкретної задачі фіксовані значення $L_\nu(f)$, $\nu = \overline{1,n}$ на фіксованій сітці вузлів X_j, $j = \overline{1,N}$), клас F_N звуть інтерполяційним, $F_{N,\varepsilon}$ – інтерполяційний клас F_N з наближено заданою вихідною інформацією. Саме класи $F_{N,\varepsilon}$ найкращим чином описують конкретні задачі.

Занурення задачі у більш вузькі класи дають змогу покращити потенційну спроможність чисельного методу.

Для побудови оптимальних квадратурних та кубатурних формул для класу F використовують метод "капелюхів", а для класів F_N та $F_{N,\varepsilon}$ "метод граничних функцій" [2].

Оптимальні оцінки цих алгоритмів [2] враховують похибку методу (для класів F, F_N) або методу і неусувну (для класу $F_{N,\varepsilon}$).

В реальному обчислювальному процесі присутня ще похибка заокруглення, яку треба дослідити для оптимальних за точністю алгоритмів. При великих розмірностях задачі вона може вносити значний вклад в оцінку повної похибки [2] обчислювального алгоритму. Аналіз оцінки похибки заокруглення може підказати необхідність переходу на s-слівну арифметику [3].

Тільки оцінка повної похибки обчислювального алгоритму може дати гарантію якості наближеного розв'язку задачі. Тому оцінки похибки заокруглення мають таку ж, якщо не більшу (особливо для задач великої розмірності відносно n і N) вагу поряд з похибкою методу та неусувної похибками.

Як приклад наведемо оцінку похибки заокруглення для оптимальної квадратурної формули типу "середньої точки"

$$R(\omega) = \sum_{\nu=0}^{N-1} f_\nu \int_{x_{\nu-1/2}}^{x_{\nu+1/2}} \sin \omega x dx \qquad (4)$$

обчислення інтегралу (3) при $g(x) = \sin \omega x$ і $F \equiv C_{L,N}$ (інтерполяційний клас Ліпшиця).

Оцінка похибки заокруглення оптимальної за точністю квадратної формули для режиму плаваючої коми та класичному правилу заокруглення, має вигляд [5]

$$\varepsilon_з \le 2^{-\tau_1}\left\{N\left(|f_0|+\frac{L}{2}\right)+|\omega|\left(|f_0|+L+|f_{N-1}|\right)+\delta\left(|f_0|+L+|f_{N-1}|\right)+2|f_0|+\frac{7}{2}L+3|f_{N-1}|\frac{|\omega|+\delta+4}{N}L\right\},$$

де $\tau_1=\tau-\log_2(1{,}06)=\tau-0{,}08406$, $\delta>0$ кількість операцій підпрограми обчислення синуса (косинуса), τ – кількість двійкових розрядів у мантиси числа.

3. Розв'язання задач цифрової обробки сигналів (ЦОС). Обчислення дискретного перетворення Фур'є

Тут і далі покажемо, як врахування оцінок похибки заокруглення допомагає у створенні T -ефективних алгоритмів розв'язання ряду важливих задач прикладної математики:

– ЦОС;
– комп'ютерної стеганографії;
– обчислення криптопримітивів.

Почнемо з деяких задач ЦОС:

– обчислення дискретних ортогональних перетворень;
– обчислення оцінок авто і взаємно кореляційних функцій стаціонарних ергодичних процесів;
– обчислення оцінок авто і взаємно спектральних щільностей випадкових процесів.

Якщо для обчислення (3) прийняти $n=1$, $\Omega=[a,b]$, $g(x)=e^{-i\omega x}$, $x_\nu=\nu\cdot\Delta x$, $\omega_k=k\cdot\Delta\omega=k\cdot 2\pi\cdot\Delta f$, $\Delta f=\dfrac{1}{b-a}$, $f(x_\nu)=f_\nu$, $\omega_N=e^{-i2\pi/N}$, то отримаємо

$$R(k)\approx\Delta t\sum_{\nu=0}^{N-1}f_\nu\cdot W_N^{k\nu}. \qquad (5)$$

Співвідношення (5) визначає дискретне перетворення Фур'є (ДПФ) функції $f(x)$. $R(k)$ звуться коефіцієнтами ДПФ.

Для обчислення (5) доцільно використовувати алгоритми швидкого перетворення Фур'є (ШПФ), Віноградa, Z -перетворення та інші швидкі ортогональні перетворення [6].

Алгоритм Віноградa, запропонований у 1976 році для обчислення ДПФ, застосовується у випадку коли N є добутком взаємно простих співмножників із набору $\{2,3,4,5,7,8,9,16\}$. В основі алгоритму лежить ідея ефективного обчислення ДПФ малої довжини, китайська теорема про лишки і методи «гніздування» обчислень [6].

Алгоритм швидкого Z -перетворення [6] має вигляд

$$U(k)=\Delta t\sum_{\nu=0}^{N-1}f(\nu)\cdot z_k^{-\nu},\ z\ne 0,\ k=\overline{0,M-1}:\ z_k=A\cdot W^{-k},$$

де A, W – комплексні константи, $M\ne N$.

ШПФ є частинним випадком Z -перетворення, коли $A=1$, $M=N$, $W_N=e^{-i2\pi/N}$.

В порівнянні із ШПФ алгоритм швидкого Z -перетворення більш гнучкий. Він дозволяє обчислювати ДПФ у випадках, коли N не є добутком багатьох співмножників при $M\ne N$. Крім того, точки Z_k можуть розташовуватись на спіралі (а не на крузі) і не обов'язково бути рівномірно розташованими.

Для оптимізації обчислення ДПФ можна також розглядати ДПФ в інших базах (Уолша, Віленкіна – Крестенсона (ВКФ), Хаара й інші) з наступним переходом у базис Фур'є [6].

Пряме обчислення ДПФ (5) потребує порядку N^2 операцій множення та N^2 додавань комплексних чисел. Набір алгоритмів, які називаються алгоритмами ШПФ, включає різноманітні засоби зменшення часу обчислення ДПФ.

Оскільки обчислення ДПФ є основною операцією в багатьох задачах ЦОС, використання ШПФ та інших швидких ортогональних перетворень (ШОП), що дозволяють на два, три порядка прискорити обчислення ДПФ у порівнянні з стандартними методами, має надзвичайно важливе значення. Асимптотично перевага ШПФ така, що для великих N (задачі трансобчислювальної складності) кількість операцій алгоритму ШПФ складає 1% від кількості операцій стандартного алгоритму.

Оцінки знизу кількості операцій комплексного додавання $Q^{+}_{\text{ДПФ}}$ і кількості «операцій» $Q^{o}_{\text{ДПФ}}$ (під «операцією» розуміється комплексне множення, за яким виконується комплексне додавання) для обчислення ДПФ комплексного сигналу на множині лінійних алгоритмів при $N = 2^{\gamma}$, $\gamma > 0$ – ціле, мають вигляд

$$Q^{+}_{\text{ДПФ}} > \frac{N}{2}\log N, \tag{6}$$

$$Q^{o}_{\text{ДПФ}} > \frac{N}{2}\log N. \tag{7}$$

Алгоритм Ш. Віноградa потребує приблизно такої ж кількості операцій додавання, що й алгоритм ШПФ, а кількість операцій множення складає $O(N)$.

В роботі [2] наведена модифікація алгоритму ШПФ $\left(\bar{A}\right)$ з попереднім обчисленням необхідних елементів матриці перетворення $W:\left\{W_N^{kj}\right\}k, j=\overline{0, N-1}$. Алгоритм $\bar{A}$ використовує такі резерви оптимізації обчислень ШПФ:

– обсяг інформації про необхідні елементи матриці зменшений в $2N$ разів;

– необхідні елементи W подані у вигляді, що не залежать від N (від N залежить лише їх кількість);

– вибірка необхідних елементів W максимально спрощена;

– здійснено більш глибоке (в порівнянні з розпаралелюванням алгоритму по «метеликам») подальше його розпаралелювання в залежності від складності його базової операції;

– алгоритм $\bar{A}$ дозволяє не враховувати $O\left(N^2\right)$ операцій, необхідних для обчислення елементів матриці W і дає можливість зробити реальним прискорення обчислювального процесу в $N/\log_2 N$ разів у порівнянні зі стандартним алгоритмом.

Для алгоритму $\bar{A}$ справедливі співвідношення:

$$Q^{+}_{ДПФ}\left(\bar{A}\right)=\left[\frac{N\log_2 N}{2}-\frac{5N}{3}+8\right], \tag{8}$$

$$Q^{o}_{ДПФ}\left(\bar{A}\right)=\left[\frac{N\log_2 N}{2}-\frac{13N}{8}+\frac{5}{8}\right], \tag{9}$$

де $[a]$ – ціла частина числа a.

Порівняння оцінок (6), (7) з (8), (9) показує, що запропоноване розпаралелювання базових операцій ШПФ безумовно себе виправдовує. Треба зазначити, що оцінки проводились за різними наборами базових операцій (шляхом урахування їхньої різної складності).

Шляхи подальшої оптимізації обчислень ДПФ наступні:

– використання різних основ алгоритму ШПФ (4, 4+2, 8);

– розгляд ДПФ в інших базисах (Уолша, ВКФ, Хаара тощо) з наступним переходом у базис Фур'є;

– використання різних режимів обчислень і різних моделей обчислень;

– використання ШПФ разом з іншими типами ШОП (Z -перетворень, теоретико-числових перетворень тощо).

Оскільки ШПФ – основний алгоритм, який використовується під час розв'язання задач ЦОС, то для задач трансобчислювальної складності суттєвим стає дослідження оцінок похибки заокруглення алгоритму ШПФ та інших T -ефективних алгоритмів розв'язання задач ЦОС, які використовують алгоритм ШПФ.

У зв'язку з цим розглянемо детерміновані та ймовірнісні оцінки похибки заокруглення алгоритму ШПФ для режимів плаваючі та фіксованої ком.

Перш за все зауважимо, що, як показано в [6], для отримання апостеріорної оцінки похибки заокруглення алгоритму ШПФ може бути використаний сам алгоритм ШПФ.

Наведемо детерміновану оцінку похибки заокруглення для обчислення n-вимірного ДПФ (у випадку, коли елементи матриці W обчислені наближено):

$$R\left(k_1,k_2,...,k_n\right)=\sum\sum...\sum\exp\left(\frac{\nu_1k_1}{N_1}+\frac{\nu_2k_2}{N_2}+...+\frac{\nu_nk_n}{N_n}\right)\cdot f\left(\nu_1,\nu_2,...,\nu_n\right),$$

де $\nu_ik_i=\overline{0,N_i-1},\ i=\overline{1,n}$.

Нехай

$$\varepsilon_з\left(k_1,k_2,...,k_n\right)=fl\left(R\left(k_1,k_2,...,k_n\right)\right)-R\left(k_1,k_2,...,k_n\right),$$

$$\left\|\varepsilon_з\right\|_E=\left\{\sum_{k_1}\sum_{k_2}...\sum_{k_n}\left|E\left(k_1,k_2,...,k_n\right)\right|^2\right\}^{1/2},$$

$$\left\|\varepsilon_з\right\|_1=\max_{k_1,k_2,...,k_n}\left|E\left(k_1,k_2,...,k_n\right)\right|.$$

Тоді

$$\left\|\varepsilon_з\right\|_E\le\left[\varepsilon_1\sum_{i=1}^{n}k\left(N_i,\delta\right)+O\left(\varepsilon_1{}^2\right)\right]\cdot\left\|R\right\|_E, \tag{10}$$

$$\left\|\varepsilon_з\right\|_1\le\left[\varepsilon_1\left(N_1,N_2,...N_n\right)^{1/2}\sum_{i=1}^{n}k\left(N_i,\delta\right)+O\left(\varepsilon_1{}^2\right)\right]\cdot\frac{1}{\left(N_1,N_2,...N_n\right)^{1/2}}\left\|R\right\|_E, \tag{11}$$

$k\left(N,\delta\right)=\sum_{j=1}^{\nu}\alpha\left(N_j\right)+\left(\gamma-1\right)\left(3+2\delta\right)$ і $\alpha\left(N_j\right)=\sqrt{2}$ при $N_j=2$, $\alpha\left(N_j\right)=5$ при $N_j=4$, $\alpha\left(N_j\right)=2\sqrt{N_j\left(N_j+\delta\right)}$ в інших випадках; $\varepsilon_1=2^{-\tau}$, обчислення ведуться з плаваючою комою; δ залежить від способу обчислення синусів і косинусів і їх аргументів і не залежить від вхідних даних, $N=N_1\cdot N_2\cdot...\cdot N_\nu$.

Оцінки (10), (11) використовуються при цифровій обробці зображень.

В роботі [7] для рандомізованого правила заокруглення і сигналу «білого» шуму отримано співвідношення для відношення дисперсії похибки заокруглення до дисперсії вектора ДПФ:

$$\frac{\delta^2_{\varepsilon_з}}{\delta^2_R} = 0.21 \cdot \nu \cdot 2^{-2\tau}. \tag{12}$$

При відсіченні результатів у правій частині (12) буде не лінійна залежність від ν, а квадратична.

В роботі [8] для детермінованого сигналу $|f(t)| < 1/2$, рандомізованого правила заокруглення і обчислень у режимі фіксованої коми має місце наступна двостороння оцінка:

$$(\nu - 2{,}5)c^2 \cdot 2^{-2\tau} \le \frac{\delta^2_{\varepsilon_з}}{\delta^2_R} \le 2^{\nu+2} \cdot 2^{-2\tau} \cdot c^2 / \sqrt{K}, \tag{13}$$

де $K = \frac{1}{N}\sum_{t=0}^{N-1} |f(t)|^2$; $c = 0{,}3$ для заокруглення, $c = 0{,}4$ для відсічення результатів операції.

Одне з найбільш важливих застосувань алгоритму ШПФ пов'язано з використанням теореми про згортку двох дискретних функцій і застосуванням її до розв'язання задач кореляційного і спектрального аналізу стаціонарних ергодичних випадкових процесів – двох важливих класів задач ЦОС. Алгоритми, які в результаті отримуються, належать до класу T -ефективних алгоритмів [9]. На практиці мінімальна вибірка сигналів, що обробляються порядку $2^{16} - 2^{17}$ відліків. Як бачимо, навіть при мінімальній вибірці похибка заокруглення відповідних алгоритмів може бути значною – особливо при правилі заокруглення – відсічення. Тому для отримання ε -розв'язків задачі, треба мати оцінки похибок заокруглення і враховувати їх у відповідних комп'ютерних технологіях розв'язання задач ЦОС [10].

У зв'язку з цим, розглянемо деякі T -ефективні алгоритми розв'язання задач кореляційного та спектрального аналізу та відповідні їм оцінки похибки заокруглення.

Оцінка взаємно кореляційної функції $R_{xy}(\tau)$ центрованих стаціонарних ергодичних випадкових процесів $x(t)$, $y(t)$, заданих на $[0,T]$ має вигляд

$$R^*_{xy}(j) = R^*_{xy}(j\Delta\tau) = \frac{1}{N-j}\sum_{k=0}^{N-j-1} x_k \cdot y_{k+j},\ j = \overline{L-1}, \tag{14}$$

де $x(t_n) = x_n$, $y(t_n) = y_n$, $k = \overline{0, N-1}$ – дійсні значення випадкових процесів $x(t)$, $y(t)$ у вузлах $t_k = k \cdot \Delta t$, $\Delta t = T/N$.

Прискорений алгоритм обчислення (14) ґрунтується на використанні теореми про згортку двох послідовностей (непрямий метод)

$$x'_k = \begin{cases} x_k, \overline{k = 0, N-1}, \\ 0, k = \overline{N, N_1 - 1}; \end{cases} \qquad y'_k = \begin{cases} y_k, \overline{k = 0, N-1}, \\ 0, k = \overline{N, N_1 - 1}, \end{cases} \tag{15}$$

де $N_1 \ge N + L$, $N_1 = 2^\gamma$.

Тут алгоритм ШПФ використовується тричі: для обчислення ДПФ послідовностей x'_k і y'_k, $k = \overline{0, N_1 - 1}$ та оберненого ДПФ добутку ДПФ x'_k, y'_k. «Набивка» нулями в (15) пов'язана з ліквідацією так званої міжперіодичної інтерференції [11].

Оцінка евклідової норми похибки заокруглення обчислення (14) непрямим методом має вигляд [2]:

$$\left\| fl\left(R^*_{xy}\right) - R^*_{xy} \right\|_E < 8 \cdot 1{,}06\sqrt{N_1} \cdot \gamma \cdot 2^{-\tau} \|x\|_E \cdot \|y\|_E. \tag{16}$$

Для обчислення оцінки взаємної спектральної щільності $S_{xy}(f)$ використаємо метод прямого перетворення Фур'є з використанням алгоритму ШПФ:

$$S^*_{xy}(f_k) = \frac{h}{N}\hat{x}^*_k \cdot \hat{y}_k, \tag{17}$$

де $\hat{x}, \hat{y}$ – ДПФ вибірок стаціонарних ергодичних процесів з нульовими середніми значеннями $x(t)$ і $y(t)$ відповідно; $\hat{x}^*_k$ величина, комплексно спряжена до $\hat{x}_k$.

Оцінка евклідової норми похибки заокруглення $\varepsilon_з$ при обчисленні $S^*_{xy}(f)$ у режимі плаваючої коми з τ двійковими розрядами з мантис чисел має вигляд [2]

$$\|\varepsilon_з\|_E < 8 \cdot 1{,}06 \cdot h \cdot \gamma \cdot \sqrt{N}\left(\|x\|_E + \|y\|_E\right) \cdot \|x\|_E \cdot \|y\|_E \cdot 2^{-\tau}. \tag{18}$$

Оцінки (16), (18) використовуються в сучасних комп'ютерних технологіях при виборі параметрів відповідних алгоритмів (можливий перехід до s-слівної арифметики [3]) для отримання ε-розв'язків задач.

4. Інші класи задач

Наголосимо ще на двох класах задач, комп'ютерні технології розв'язання яких щільно використовують оцінки похибки заокруглення відповідних алгоритмів.

Перший – це багаторозрядна арифметика, яка застосовується у двоключовій криптографії, високоточних обчисленнях, під час розв'язання задач трансобчислювальної складності, боротьбі з накопиченням похибки заокруглення при отриманні ε-розв'язку задачі.

Одна з основних операцій багаторозрядної арифметики – це множення багаторозрядних чисел. Алгоритм Шенхаге – Штрассена виконання цієї операції, який є асимптотично ефективним серед інших відомих алгоритмів множення, при своїй реалізації використовує оцінку похибки заокруглення алгоритму обчислення згортки двох дискретних функцій (непрямого методу). Використовуючи цю оцінку треба настроїти параметри алгоритму такими, щоб гарантувати оцінку похибки заокруглення алгоритму множення меншою за $1/2$. Тоді отримаємо точний результат множення.

Другий – спектральні алгоритми розв'язання задач комп'ютерної стеганографії – розмістити вхідне повідомлення у цифровому («пустому») контейнері таким чином, щоб будь-яка стороння людина не змогла помітити нічого, крім основного вмісту контейнера, навіть якщо застосує додаткову статистичну обробку стеганоконтейнера.

В одному з спектральних алгоритмів, який використовує алгоритм ШПФ, будується спектр цифрового контейнера, визначаються участки спектру, які відповідають спектру шуму і в компоненти спектру шуму приховують таємне повідомлення, причому в такий спосіб, що використовує оцінку похибки заокруглення стеганоалгоритму.

Відповідні комп'ютерні технології розв'язання цих двох класів задач наведені в [10, 12].

Висновки. Показана важливість урахування оцінок похибок заокруглення у сучасних комп'ютерних технологіях розв'язання задач ЦОС, багаторозрядної арифметики, комп'ютерної стеганографії для контролю та зменшення похибки заокруглення для задач трансобчислювальної складності.

Авторські внески. Задірака В.К.: побудова стійких до похибок заокруглення обчислювальних алгоритмів (вступ, розділи 1–3). Швідченко І.В.: високоточні обчислення під час розв'язання задач трансобчислювальної складності, боротьба з накопиченням похибки заокруглення при отриманні ε-розв'язку задачі (розділи 3, 4, висновки).

Наявність даних. Дані, які підтверджують висновки цього дослідження, доступні в [5].

Фінансування. Автори не отримували фінансування для проведення досліджень та написання статті.

Список літератури

1. Задірака В.К., Швідченко І.В. ε-розв'язок задачі. Збірник матеріалів проблемно-наукової міжгалузевої конференції *"Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, моделювання та управління"* (*ICSM-2022*), *14–15 липня 2022 р*. Надвірна, 2022. С. 29–32.
2. Задирака В.К. Теория вычисления преобразования Фурье. К.: Наукова думка, 1983. 216 с.
3. Задірака В.К., Терещенко А.М. Комп'ютерна арифметика багаторозрядних чисел у послідовній та паралельній моделях обчислень. К.: Наукова думка, 2021. 136 с. https://books-nasu.org.ua/computer-arithmetics-of-multi-digits-numbers-in-sequential-and-parallel-calculation-models/
4. Sergienko I.V., Zadiraka V.K., Lytvyn O.M. Elements of the General Theory of Optimal Algorithms. Springer, 2021. 378 p. https://doi.org/10.1007/978-3-030-90908-6
5. Задірака В.К., Луц Л.В., Швідченко І.В. Теорія обчислень інтегралів від швидкоосцилювальних функцій. К.: Наукова думка, 2023. 472 с. https://doi.org/10.15407/978-966-00-1843-3
6. Задирака В.К., Мельникова С.С. Цифровая обработка сигналов. К.: Наукова думка, 1993. 294 с.
7. Weinstein C. Roundoff noise in floating point fast Fourier transform computation. *IEEE Transactions on Audio and Electroacoustics*. 1969. **17** (3). P. 209–215. https://ieeexplore.ieee.org/document/1162049
8. Welch P. A fixed-point fast Fourier transform error analysis. *IEEE Transactions on Audio and Electroacoustics*. 1969. **17** (2). P. 151–157. https://ieeexplore.ieee.org/document/1162035
9. Задірака В.К., Бабич М.Д., Березовський А.І., Бесараб П.М., Гнатів Л.О., Людвиченко В.О. *Т*-ефективні алгоритми наближеного розв'язання задач обчислювальної та прикладної математики. Київ-Тернопіль: «Збруч», 2003. 261 с.
10. Задірака В.К., Швідченко І.В. Використання похибки заокруглення в сучасних комп'ютерних технологіях. *Кібернетика та комп'ютерні технології*. 2021. № 3. С. 43–52. https://doi.org/10.34229/2707-451X.21.3.4
11. Голд Б., Рейдер К. Цифровая обработка сигналов. М.: Сов. радио, 1973. 368 с.
12. Задирака В.К., Швидченко И.В. Влияние качества оценки погрешности округления стеганоалгоритма на его стойкость. *Математичне та комп'ютерне моделювання. Серія: Фізико-математичні науки*. 2015. Вип. 12. С. 101–112. http://mcm-math.kpnu.edu.ua/article/view/52691/48742

Одержано 13.03.2024

Задірака Валерій Костянтинович,
доктор фізико-математичних наук, професор, академік НАН України, завідуючий відділом
Інституту кібернетики імені В.М. Глушкова НАН України, Київ,
https://orcid.org/0000-0001-9628-0454
zvk140@ukr.net

Швідченко Інна Віталіївна,
кандидат фізико-математичних наук, старший науковий співробітник, провідний науковий співробітник
Інституту кібернетики імені В.М. Глушкова НАН України, Київ.
https://orcid.org/0000-0002-5434-2845
inetsheva@gmail.com

УДК 519.6; 519.64

В.К. Задірака [*], І.В. Швідченко [*]

Методи боротьби з накопиченням похибки заокруглення під час розв'язання задач трансобчислювальної складності

Інститут кібернетики імені В.М. Глушкова НАН України, Київ
[*] *Листування: zvk140@ukr.net, inetsheva@gmail.com*

Вступ. Основна увага приділена необхідності врахування оцінок похибок заокруглення під час розв'язання задач трансобчислювальної складності. Серед таких задач можна виділити задачі обчислення систем лінійних алгебраїчних рівнянь з кількістю невідомих у декілька десятків мільйонів, цифрової обробки сигналів, розрахунку ядерних реакторів, моделювання фізичних, хімічних процесів, аеродинаміки, захисту інформації тощо.

Неврахування похибки заокруглення під час їх розв'язання призводить до того, що іноді отримуються комп'ютерні рішення, які не відповідають фізичному змісту задачі.

Мета статті. Показано, як, використовуючи оцінки похибок заокруглення, будувати стійкі до похибок заокруглення обчислювальні алгоритми. При цьому враховуються: правило заокруглення, режим обчислення, якість оцінок похибок заокруглення (непокращувальна оцінка, асимптотична оцінка, ймовірнісна оцінка).

За наявності обчислювальних ресурсів доцільно використовувати асимптотичні оцінки та ймовірнісні як більш точні у порівнянні з мажорантними оцінками.

Результати. Показано, як у сучасних комп'ютерних технологіях використовуються оцінки похибок заокруглення для отримання ε-розв'язку наступних задач прикладної математики:

– обчислення інтегралів від швидкоосцилюючих функцій;
– розв'язання задач цифрової обробки сигналів;
– обчислення дискретного перетворення Фур'є;
– багаторозрядна арифметика;
– комп'ютерна стеганографія.

Найбільша увага приділена *T*-ефективним алгоритмам обчислення дискретного перетворення Фур'є та розв'язанню задач спектрального і кореляційного аналізу випадкових процесів. Ці класи задач входять як складові під час розв'язання задач двоключової криптографії та комп'ютерної стеганографії.

Висновки. Показана важливість урахування оцінок похибок заокруглення у сучасних комп'ютерних технологіях розв'язання ряду класів задач обчислювальної та прикладної математики.

Ключові слова: похибка заокруглення, комп'ютерна технологія, дискретне перетворення Фур'є, інтегрування швидкоосцилюючих функцій, інформаційна безпека.

UDC 519.6; 519.64

Valerii Zadiraka [*], Inna Shvidchenko [*]

Methods of Combating the Accumulation of Rounding Error When Solving Problems of Trans-Computational Complexity

V.M. Glushkov Institute of Cybernetics of NAS of Ukraine, Kyiv
[*] Correspondence: zvk140@ukr.net, inetsheva@gmail.com

Introduction. The main attention is paid to the need to take into account estimates of rounding errors when solving problems of transcomputational complexity. Among such tasks, one can highlight the tasks of calculating systems of linear algebraic equations with the number of unknowns in the tens of millions, digital signal processing, calculating nuclear reactors, modeling physical and chemical processes, aerodynamics, information protection, etc.

Ignoring the rounding error when solving them leads to the fact that sometimes we obtain computer solutions that do not correspond to the physical content of the problem.

The purpose of the article. It is shown how, using estimates of rounding errors, to build computational algorithms resistant to rounding errors. At the same time, the following are taken into account: the rounding rule, the calculation mode, the quality of rounding error estimates (non-improving estimate, asymptotic estimate, imputed estimate).

If computing resources are available, it is advisable to use asymptotic and probabilistic estimates as they are more accurate compared to majorant estimates.

The results. It is shown how the estimates of rounding errors are used in modern computer technologies to obtain ε-solution of the following problems of applied mathematics:

– calculation of integrals from fast oscillating functions;
– solving problems of digital signal processing;
– calculating the discrete Fourier transform;
– multi-bit arithmetic;
– computer steganography.

The greatest attention is paid to *T*-effective algorithms for calculating the discrete Fourier transform and solving the problems of spectral and correlation analysis of random processes. These classes of problems are included as components in solving problems of two-key cryptography and computer steganography.

Conclusions. The importance of taking into account estimates of rounding errors in modern computer technologies for solving a number of classes of computational and applied mathematics problems is shown.

Keywords: rounding error, computer technology, discrete Fourier transform, integration of fast oscillating functions, information security.