КІБЕРНЕТИКА та КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ

УДК 519.65 DOI:10.34229/2707-451X.21.3.4

В.К. ЗАДІРАКА, І.В. ШВІДЧЕНКО

ВИКОРИСТАННЯ ПОХИБКИ ЗАОКРУГЛЕННЯ В СУЧАСНИХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЯХ

Показана важливість врахування похибок заокруглення в сучасних комп'ютерних технологіях розв'язання задач обчислювальної та прикладної математики з заданими значеннями характеристик якості за точністю та швидкодією. Розглянуті наступні класи задач: розв'язання систем лінійних алгебраїчних рівнянь, задач цифрової обробки сигналів, задач комп'ютерної стеганографії та використання багаторозрядної арифметики для контролю та зменшення похибки заокруглення при розв'язанні задач трансобчислювальної складності.

Ключові слова: *похибка заокруглення, комп'ютерні технології, дискретне перетворення Фур'є, багаторозрядна арифметика, комп'ютерна стеганографія.*

Вступ. Похибка заокруглення – одна з видів похибок, яка разом зі спадковою похибкою і похибкою методу, впливає на точність наближеного розв'язку задач.

Якщо до 60-х років похибкою заокруглення нехтували (вважали її значно менше за інші види похибок), то в подальшому завдяки роботам Дж.Х. Вілкінсона, В.В. Воєводіна та інших вчених і збільшенні складності задач, що розв'язуються, їй почали приділяти значну увагу.

Найбільш досліджуваним класом задач з точки зору накопичення похибки заокруглення була лінійна алгебра, але потім методи теорії похибок заокруглення почали використовуватися і для інших класів задач.

Кожна арифметична операція вносить свій «внесок» в оцінку похибки заокруглення. І чим більше операцій, тим більший цей «внесок». При розв'язанні задач трансобчислювальної складності неврахування похибки заокруглення призводить до того, що отримані комп'ютерні моделі досліджуваних явищ нічого спільного з фізичними моделями не мають. Для таких класів задач часто похибка заокруглення стає самою значущою – її «внесок» в оцінку повної похибки обчислювального алгоритму стає значним, і не враховувати його не тільки не можна, але й неврахування її не дає можливості отримати ε -розв'язок задачі.

Проаналізуємо різні правила заокруглення: класичне, відсікання і рандомізоване. Саме задачі АСУ та комп'ютерна техніка ЄС ЕОМ «підштовхнули» електронників перейти від класичного правила заокруглення до відсікання (оскільки схемно дуже просто реалізується і задачі АСУ мали відносно невелику складність). Якщо розташувати зазначені правила заокруглення в порядку накопичення похибки заокруглення, то найповільніше похибка заокруглення накопичується при рандомізованому правилі заокруглення, потім йде класичне правило і найгірше – відсікання.

Незважаючи на критику математиків на адресу відсікання, електронники не можуть відійти від простоти його реалізації і, як ми бачимо, і в персональних ЕОМ і навіть у суперкомп'ютерах залишається відсікання.

Ми «женемося» за швидкодією, забуваючи про точність, і про те, що час, точність і використовувана пам'ять комп'ютера взаємопов'язані.

Основними постановками задач оптимізації обчислень є:

– мінімізація часу $T(I,X,Y)$ при дотриманні реальних (Re) обмежень на точність $E(I,X,Y)$ і пам'ять $M(I,X,Y)$:

$$T(I,X,Y)=\min_{I,X,Y},\ E(I,X,Y)\le E_{\mathrm{Re}},\ M(I,X,Y)\le M_{\mathrm{Re}}, \tag{1}$$

– мінімізація повної похибки $E(I,X,Y)$ при дотриманні обмежень на T і M

$$E(I,X,Y)\le \min_{I,X,Y},\ T(I,X,Y)=T_{\mathrm{Re}},\ M(I,X,Y)\le M_{\mathrm{Re}}, \tag{2}$$

де I,X,Y – скінченні множини параметрів, від яких істотно залежать відповідно задача, алгоритм, комп'ютер.

Неврахування обмежень може призвести до абсурдних постановок задач і результатам, отриманими в рамках таких постановок. Наприклад, якщо в (1) не враховувати обмеження на $E(I,X,Y)$, то можна стверджувати, що оптимальний за швидкодією алгоритм вимагає час рівний часу вибірки числа з пам'яті комп'ютера.

T,E,M як правило, нам невідомі, але нам відомі їхні оцінки $\tilde{T},\tilde{E},\tilde{M}$. Оцінки можуть бути апріорними, апостеріорними, мажорантними, асімтотичними, детермінованими, статистичними. Мажорантні оцінки, які найбільш часто використовуються, можуть бути різної якості: грубі і непокращувальні. З точки зору математичного аналізу, теорії функцій, наприклад, непокращувальні оцінки точності – це суперрезультати. Але на практиці задачі, на які вони досягаються (або асимптотично досягаються), не зустрічаються, хоча формально належать класу задач, що розглядається. Так що непокращувальні оцінки на практиці є завищеними (для реальних задач).

Як бути? Є два способи. Перший – це «занурити» задачу в більш вузький клас (звужувати до тих пір, поки непокращувальні оцінки не будуть досягатися на реальних задачах). В цьому випадку оцінкам можна «довіряти». Це важливо, оскільки на їх підставі визначаються оцінки обчислювальних ресурсів, необхідних для розв'язання задач (1), (2), а також вони використовуються в комп'ютерних технологіях розв'язання задач обчислювальної і прикладної математики із заданими значеннями характеристик якості за точністю і швидкодією. Другий шлях – вважати вектор I випадковим і знаходити статистичні оцінки характеристик. Статистичні характеристики краще відображають поведінку похибок для задач середньої складності.

Важливе значення має отримання асимптотичних оцінок похибок, які знаходяться порівняно просто за рахунок врахування малих величин лише головних порядків і які поблизу граничних значень варійованих параметрів виявляються близькими до реальних похибок.

Нагадаємо, що використовуються два режими обчислень – плаваюча кома та фіксована. Оцінки похибки заокруглення безумовно різні. Режим фіксованої коми дозволяє пришвидшити обчислювальний процес (не треба вирівнювати порядки) але за рахунок втрати точності. Режим плаваючої коми дозволяє здійснювати більш точні розрахунки але при цьому час розв'язку задачі збільшується в порівнянні з фіксованою комою. Вибір режиму обчислень здійснюється на основі обмежень в (1), (2) на T і E.

Наведемо оцінки похибок заокруглення алгоритмів розв'язання деяких найбільш поширених задач обчислювальної, прикладної математики та захисту інформації.

1. Оцінка середнього для нормального розподілу

Нехай x – випадкова величина з областю значень $[a,b]$, $-\infty\le a<b\le\infty$; $p(x)$ – щільність розподілу x. Математичним очікуванням або середнім значенням x називається число $\bar{x}\equiv M_x\equiv M(x)=\int_a^b xp(x)dx$.

А. Оцінка в режимі off-line. Нехай в пам'яті комп'ютера є вибірка з N значень, які позначимо $x_\nu, \nu=\overline{1,N}$. Зазвичай за оцінку $\bar{x}$ приймають вибіркове середнє

$$S_N \equiv \bar{x}^* \equiv M_x^* \equiv M^*(x) = \frac{1}{N}\sum_{\nu=1}^{N} x_\nu . \tag{1}$$

Оцінимо похибку заокруглення при обчисленні на комп'ютері за формулою (1). Будемо припускати, що обчислення виконуються в режимі плаваючої коми з τ розрядами у мантис чисел.

При обчисленні на комп'ютері співвідношення (1) набуде вигляду:

$$(S_N)_\tau = \left(\sum_{\nu=1}^{N} x_\nu\right)_\tau (:)_\tau N \equiv \frac{1}{N}\sum_{\nu=1}^{N} x_\nu (1+E_\nu),$$

де індекс τ означає заміну відповідних операцій на псевдооперації з заокругленням результатів арифметичних операцій, а

$$|E_\nu| \le 1{,}06(N-\nu+2)\cdot 2^{-\tau},\ N\cdot 2^{-\tau} < 0{,}1,\ \nu=\overline{1,N}.$$

Детермінована мажорантна оцінка похибки заокруглення має вигляд [1]:

$$|S_N - (S_N)_\tau| \le \frac{1}{N}\sum_{\nu=1}^{N}|x_\nu||E_\nu| \le \frac{1{,}06}{\sqrt{3}}\sqrt{\left(1-\frac{1}{2N}\right)\left(1-\frac{1}{N}\right)\frac{1}{N}\sum_{\nu=1}^{N}x_\nu^2}\cdot 2^{-\tau},\ N\cdot 2^{-\tau} < 0{,}1.$$

Б. Оцінка в режимі on-line. Нехай в пам'ять комп'ютера надходять наближені значення x_ν випадкової величини x і потрібно отримати значення S_N в темпі надходження $x_\nu, \nu=\overline{1,N}$, з мінімальною витратою пам'яті комп'ютера. Цього можна досягти застосуванням формули

$$S_i = \frac{i-1}{i}S_{i-1} + \frac{x_i}{i},\quad i=\overline{1,N},\ S_0 = 0. \tag{2}$$

Для співвідношення (2) будемо мати з точністю до перших ступенів $2^{-\tau}$ [1]:

$$|S_N - (S_N)_\tau| \le (3N+7)\cdot 2^{-\tau-1}\cdot \max_{1\le\nu\le N}|x_\nu| .$$

2. Розв'язання систем лінійних алгебраїчних рівнянь

Наведемо зведення апріорних асимптотичних детермінованих і статистичних оцінок похибок заокруглення для основних прямих методів розв'язання систем лінійних алгебраїчних рівнянь n-го порядку

$$Ax = y,$$

для яких матриця A має обернену матрицю A^{-1}. Оцінки мають вигляд (в режимі плаваючої коми з τ розрядами у мантис і з накопиченням суми парних добутків) [2]:

$$\frac{\|x - x_\tau\|}{\|x\|} \le 2^{-\tau}\cdot f(n)\cdot \rho(A)$$

і

$$\left[M\left(\frac{\|x-x_\tau\|^2}{\|x\|^2}\right)\right]^{\frac{1}{2}} \le 2^{-\tau}\cdot\varphi(n)\cdot\left[M\left(\rho^2(A)\right)\right]^{\frac{1}{2}},$$

де x_τ – розв'язок, отриманий на комп'ютері, а

$$\rho(A) = \|A\|_E \left\|A^{-1}\right\|_E .$$

Для методу Гаусса з вибором головного елемента по стовпцю

$$f(n)=3q(n+1),\ \varphi(n)=\left(\frac{2}{3}(n+1)\right)^{\frac{1}{2}},\ 1\le q\le 2^n.$$

Для методу відображень

$$f(n)=3{,}35n,\ \varphi(n)=\left(\frac{4}{3}(n+1)\right)^{\frac{1}{2}}.$$

Для методу квадратного кореня

$$f(n)=1,\ \varphi(n)=\frac{5}{3}.$$

Для методу обертань (оптимального виключення)

$$f(n)=12n,\ \varphi(n)=n^{1/2}.$$

Для методу ортогоналізації (з процедурою доортогоналізації)

$$f(n)=1,\varphi(n)=1.$$

Наведені співвідношення справедливі з урахуванням малих щодо першого порядку відносно $1/n$ і $2^{-\tau}$.

3. Обчислення дискретного перетворення Фур'є

Розглянемо задачу наближеного обчислення перетворення Фур'є фінітної з носієм $[0,T]$ функції $f(t)$:

$$F(\omega)=\int_0^T f(t)e^{-i\omega t}dt$$

у випадку, коли $f(t)$ на $[0,T]$ задана в N точках рівномірної сітки $\left(\Delta t=\frac{T}{N}\right)$.

Застосувавши для наближеного обчислення $F(\omega)$ формулу прямокутників і використавши крок за частотою $\omega_r=r2\pi\Delta f$, $\Delta f=\frac{1}{T}$ (частота Найквіста), отримаємо:

$$F(\omega_r)\approx F_N(\omega_r)=F(r)=\Delta t\sum_{k=0}^{N-1}f(k)e^{-i\frac{2\pi}{N}rk},\ f(k)=f(t_k). \tag{3}$$

Зробивши заміну $W_N=e^{-i\frac{2\pi}{N}}$, отримаємо:

$$F(r)=\Delta t\sum_{k=0}^{N-1}f(k)W_N^{rk},\ r=\overline{0,N-1}. \tag{4}$$

Співвідношення (4) визначає дискретне перетворення Фур'є (ДПФ) функції $f(t)$, $F(r), r=\overline{0,N-1}$ називаються коефіцієнтами ДПФ.

У векторно-матричній формі співвідношення (4) має вигляд

$$\left[F(r)\right]=\left[W_N^{rk}\right]\cdot\left[f(k)\right], \tag{5}$$

де $\left[F(r)\right]$ и $\left[f(k)\right]$ – вектор-стовпці $(N\times 1)$, а $\left[W_N^{rk}\right]$ – квадратна матриця порядку $(N\times N)$.

Як видно зі співвідношення (5) стандартний метод визначення вектору коефіцієнтів ДПФ вимагає N^2 операцій комплексного множення і стільки ж операцій комплексного додавання (віднімання). Прискорений метод обчислення $\left[F(r)\right], r=\overline{0,N-1}$ (швидкого перетворення Фур'є – ШПФ), який заснований на факторизації матриці $\left[W_N^{rk}\right], k,r=\overline{0,N-1}$, потребує порядку $N\log_2 N$ операцій комплексного додавання (віднімання) і порядку $\frac{N}{2}\log_2 N$ операцій комплексного множення. Порядок коефіцієнта прискорення $\frac{N}{\log_2 N}$ показує, що ми прискорюємося на кілька порядків. Це особливо важливо для задач великої розмірності і для забезпечення обробки інформації в режимі on-line. Можна вказати таке число N_0, що для $N>N_0$ кількість операцій алгоритму ШПФ становитиме лише 1% від кількості операцій стандартного методу.

Цим пояснюється широкий спектр застосувань алгоритму ШПФ. Можна назвати класи задач, в яких алгоритм ШПФ «добре впровадився». Це цифрова обробка сигналів та зображень, прикладна статистика, аналіз сейсмограм землетрусів, ядерна спектроскопія, розв'язання крайових задач для рівнянь у частинних похідних, моделювання систем автоматичного регулювання та ін.

Нас буде цікавити питання порівняльного аналізу стандартного алгоритму і ШПФ не тільки за складністю, а й за похибкою заокруглення.

Нехай обчислення проводяться на комп'ютері в режимі з плаваючою комою з τ двійковими розрядами у мантис чисел. Наведемо лему Дж.Х. Вілкінсона [3], яка нам знадобиться.

Лема. Якщо A – дійсна $(p\times q)$-матриця і B – дійсна $(q\times r)$-матриця, а $fl(\cdot)$ позначає результат обчислення виразу, що стоїть в дужках, то

$$\left\| fl(AB)-AB\right\|_E < 1{,}06\cdot 2^{-\tau}\cdot q\cdot \|A\|_E\cdot\|B\|_E .$$

На підставі цієї леми можна отримати наступні оцінки похибки заокруглення стандартного алгоритму і ШПФ:

для стандартного методу

$$\|\varepsilon\|_E < c\cdot(2N)^{3/2}, \tag{6}$$

для ШПФ при $N=N_1\cdot N_2 ... N_\nu$

$$\|\varepsilon\|_E < c\cdot\sum_{i=1}^{\nu}\left(2N_j\right)^{3/2}; \tag{7}$$

для ШПФ при $N=2^\nu$

$$\|\varepsilon\|_E < 8c\cdot\nu, \tag{8}$$

де $\varepsilon = fl(F)-F$, $c=1{,}06\cdot 2^{-\tau}\cdot\|F\|_E$.

Порівнюючи оцінку (6) з оцінками (7), (8), бачимо, що алгоритм ШПФ не тільки зменшує оцінку складності задачі обчислення коефіцієнтів ДПФ, а й істотно зменшує оцінку похибки заокруглення. Не завжди зменшення кількості операцій веде до зменшення оцінки похибки заокруглення, але для алгоритму ШПФ це так.

Наведемо оцінки $\|\varepsilon\|_E$ в припущенні, що елементи матриці W обчислені наближено:

$$fl\left(\sin\left(fl(\alpha)\right)\right)=\sin\alpha+\delta\theta\varepsilon_1,\quad fl\left(\cos\left(fl(\alpha)\right)\right)=\cos\alpha+\delta\theta\varepsilon,$$

де $\delta \geq 0$ – абсолютна константа, $-1 \leq \theta \leq 1$, $\varepsilon_1 = 2^{-\tau}$, обчислення ведуться в режимі з плаваючою комою. Константа δ залежить від способу обчислення синусів і косинусів і їх аргументів і не залежить від вхідних даних. Оцінки при $N = N_1 ... N_\nu$ мають вигляд

$$\|\varepsilon\|_E < \left[k(N,\delta)\varepsilon_1 + O\left(\varepsilon_1^{\,2}\right) \right] \cdot \|F\|_E ;$$

$$\|\varepsilon\|_1 \leq \left[\sqrt{N} k(N,\delta)\varepsilon_1 + O\left(\varepsilon_1^{\,2}\right) \right] \frac{1}{\sqrt{N}} \cdot \|F\|_E ,$$

де $k(N,\delta) = \sum_{j=1}^{\nu} \alpha(N_j) + (\gamma - 1)(3 + 2\delta)$ і $\alpha(N_j) = \sqrt{2}$ при $N_j = 2$, $\alpha(N_j) = 5$ при $N_j = 4$, $\alpha(N_j) = 2\sqrt{N_j (N_j + \delta)}$ в інших випадках.

Для алгоритмів ШПФ за основами 2 і 4

$$k(2^\nu, \delta) = \left(3 + \sqrt{2} + 2\delta\right)\nu - (3 + 2\delta) \text{ і } k(4^\nu, \delta) = (8 + 2\delta)\nu - (3 + 2\delta).$$

У разі обчислення багатовимірного ДПФ:

$$F(t_1, t_2, ..., t_m) = \sum_{s_1} \sum_{s_2} ... \sum_{s_m} \exp\left(\frac{s_1 t_1}{N_1} + \frac{s_2 t_2}{N_2} + ... + \frac{s_m t_m}{N_m} \right) \cdot f(s_1, s_2, ..., s_m),$$

де $s_i, t_i = \overline{0, N_i - 1}$, $i = \overline{1, m}$, наведемо оцінки похибок заокруглення алгоритму ШПФ.

Нехай

$$E_1(t_1, t_2, ..., t_m) = fl\left(F(t_1, t_2, ..., t_m)\right) - F(t_1, t_2, ..., t_m),$$

$$\|E_1\|_E = \left\{ \sum_{t_1} \sum_{t_2} ... \sum_{t_m} \left| E_1(t_1, t_2, ..., t_m) \right|^2 \right\}^{1/2},$$

$$\|E_1\|_1 = \max_{t_1, t_2, ..., t_m} \left| E_1(t_1, t_2, ..., t_m) \right|.$$

Тоді

$$\|E_1\|_E \leq \left[\varepsilon_1 \sum_{i=1}^{m} k(N_i, \delta) + O\left(\varepsilon_1^{\,2}\right) \right] \cdot \|F\|_E ,$$

$$\|E_1\|_1 \leq \left[\varepsilon_1 (N_1, N_2, ... N_m)^{1/2} \sum_{i=1}^{m} k(N_i, \delta) + O\left(\varepsilon_1^{\,2}\right) \right] \cdot \frac{1}{(N_1, N_2, ... N_m)^{1/2}} \|F\|_E .$$

В роботі [5] для сигналу $f(t)$ у вигляді «білого» шуму при певних обмеженнях для рандомізованого правила заокруглення отримано наступний вираз для відношення дисперсії похибки заокруглення до дисперсії вектора ДПФ:

$$\frac{\sigma_{E_\nu}^2}{\sigma_F^2} = 0,21 \cdot \nu \cdot 2^{-2\tau}. \qquad (9)$$

При відсіченні результатів у правій частині (9) буде не лінійна залежність від ν, а квадратична.

У разі детермінованого сигналу $|f(t)| < \frac{1}{2}$, рандомізованого правила заокруглення і обчислень в режимі фіксованої коми має місце наступна двостороння оцінка:

$$(\nu-2,5)c^2\cdot 2^{-2\tau}\le\frac{\sigma^2_{E_\nu}}{\sigma^2_F}\le 2^{\nu+2}\cdot 2^{-2\tau}/\sqrt{k},$$

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

4. Використання багатозарядної арифметики

Багаторозрядні числа – це числа, розрядність яких (n бітів) перевищує довжину розрядного слова. Такі числа будемо ще називати багатослівними або s-слівними.

Якщо n велике ($n>1024$ біт), то виконання операцій вимагає істотних витрат машинного часу і виникає необхідність в оптимізації за швидкодією відповідних алгоритмів і програм.

Галузь застосування таких ефективних алгоритмів – двоключова криптографія, високоточні обчислення, при розв'язанні задач трансобчислювальної складності, боротьба з накопиченням похибки заокруглення при отриманні ε-розв'язку задачі.

Стійкість деяких алгоритмів двоключової криптографії тримається на використанні саме багаторозрядних чисел (не менше 2048 бітів на одне число). І чим більша розрядність чисел, тим стійкіший алгоритм, тому що тим більше ускладнюється розв'язання задач факторизації чисел або дискретного логарифмування.

При шифруванні, розшифруванні, керуванні ключами, у криптографічних протоколах, високоточних обчисленнях використовується операція піднесення до степеня, яка є найбільш складною. Операція піднесення до степеня виконується за допомогою операції множення та піднесення до квадрату. Оскільки операція множення – ключова, то на неї лягає основне навантаження в алгоритмах двоключової криптографії. Тому зупинимось на оптимізації алгоритмів множення багаторозрядних чисел.

Відомо, що стандартний алгоритм множення вимагає $O\left(n^2\right)$ операцій для множення n-розрядних чисел. Більш якісні алгоритми можна отримати, використовуючи ідею Карацуби – Офмана та її рекурентного застосування, а також швидкі дискретні ортогональні перетворення [6]. Алгоритм Карацуби – Офмана потребує $O\left(n^{\log^2 3}\right)$ операцій, метод многочленів – $n^{1+\varepsilon}$, $(\varepsilon>0)$, алгоритм Тоома – Кука – $O\left(n\cdot 2^{\sqrt{2\log_2 n}}\right)$, алгоритм Шенхаге – Штрассена потребує $O(n\log_2 n)$ операцій. Суттєво зменшити час виконання операції множення дозволяє використання алгоритмів обчислення добутку n-розрядних чисел за модулем за допомогою добутку Монтгомері та розробка швидких алгоритмів обчислення арифметичної згортки. Усі ці алгоритми базуються на ідеї зведення множення n-розрядних чисел до множення чисел з меншою розрядністю.

С. Кук разом з С. Ондераа довели теорему про найкращу нижню границю, в якій стверджується, що за певних обмежень не існує алгоритму, який би множив n-розрядні числа менше, ніж за $O\left(\frac{n\log_2 n}{(\log_2\log_2 n)^2}\right)$ операцій.

В роботі [7] доведена асимптотична ефективність алгоритму Шенхаге – Штрассена в порівнянні з алгоритмом Карацуби – Офмана. А взагалі кожний алгоритм має область свого ефективного застосування і тому варто мати бібліотеку програм для обчислення добутку багаторозрядних чисел.

Метод множення багаторозрядних чисел з використанням ШПФ базується на ідеї використання теореми про дискретну згортку двох функцій.

Оскільки при використанні ШПФ використовуються комплексні числа W_N^{rk}, то при множенні цілих чисел ми виходимо з поля цілих чисел в поле дійсних чисел і основна кількість операцій здійснюється в полі дійсних чисел. А результат – це ціле число. Тому нам треба коректно повернутися в поле цілих чисел. Оцінка похибки заокруглення має бути меншою $\frac{1}{2}$. Тоді отримаємо точний результат. Для цього необхідно визначити число τ – кількість правильних значущих цифр, необхідних для наближеного обчислення W_N^{β}, і величин, отриманих на кожному кроці алгоритму ШПФ.

Для цього і потрібні оцінки (7)–(9). Це саме «тонке» місце алгоритму Шенхаге – Шрассена і без урахування оцінок похибок цей алгоритм не «спрацює».

Наведемо таблицю значень τ для різних N (N^2 – розмір матриці ШПФ).

ТАБЛИЦЯ. Таблиця значень τ для різних N

N	2	4	8	16	32	64	128	256	512
τ	35	40	43	44	48	51	53	55	58

Багаторозрядну арифметику можна використовувати для отримання ε-розв'язків задач трансобчислювальної складності. За Дж.Х. Вілкінсоном структура оцінок похибок заокруглення $\varepsilon_{заокр}$ має наступну структуру:

$$\varepsilon_{заокр} \le c(N) \cdot 2^{-\tau}, \tag{10}$$

де $c(N)$ – деяка функція від кількості вхідної інформації. Наприклад, в оцінці (7) $c(N) = 1{,}06 \cdot \sum_{i=1}^{\nu} \left(2N_j\right)^{3/2} \cdot \|F\|_E$.

Якщо оцінка (10) нас не задовольняє, переходимо до використання s-слівних чисел. Тоді замість оцінки (10) будемо мати

$$\varepsilon_{заокр} \le c(N) \cdot 2^{-s\tau}. \tag{11}$$

Підбором s можна намагатись отримати ε-розв'язок задачі (зауважимо, що на ε впливає також похибка методу та неусувна похибка). Для задач трансобчислювальної складності $\varepsilon_{заокр}$ може бути «головним членом». Тому s може бути тим параметром, який дозволить перевести задачу з розряду нерозв'язаної у розв'язну.

Оскільки мова йде і про багатопроцесорні комп'ютери, то актуальним є питання побудови ефективних за швидкодією алгоритмів обчислення криптопримітивів у паралельні моделі обчислень [8].

5. Застосування оцінки похибки заокруглення в алгоритмах розв'язання задач комп'ютерної стеганографії

Стеганографія – один із шляхів підтримки інформаційної безпеки. Вона являє собою метод організації зв'язку, який приховує сам факт наявності таємних повідомлень. Стеганографічні методи активно використовуються для захисту інформації від несанкціонованого доступу, для протидії системам моніторингу та керування ресурсами мереж, для маскування програмного забезпечення від незареєстрованих користувачів, а також для захисту авторського права на деякі види інтелектуальної власності. Стеганографічна система – це сукупність засобів та методів, які використовуються для формування таємного каналу зв'язку. Будь-яка інформація, в якій приховані таємні дані, називається контейнером. Контейнер, який не містить таємного повідомлення,

називають порожнім, а той, що містить – стеганоконтейнером. Канал передачі стеганоконтейнера має назву стеганографічного каналу. Таємний ключ, який необхідний для «вкраплення» інформації в контейнер, називається стеганоключем.

Задача стеганографічної системи – розмістити вхідне повідомлення в контейнері таким чином, щоб будь-яка стороння людина не змогла помітити нічого, крім його основного вмісту, навіть якщо застосує додаткову статистичну обробку стеганоконтейнера.

Актуальною є задача побудови цифрових контейнерів. Найбільш стійкими до спотворень є спектральні методи побудови стеганоконтейнерів [9], які базуються на використанні дискретних ортогональних перетворень (дискретне косинус-перетворення, Фур'є, Уолша та інші).

Не будемо заглиблюватись у теорію комп'ютерної стеганографії, а відмітимо, причому тут похибка заокруглення стеганоалгоритмів.

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.

З оцінок похибок заокруглення визначається остання правильна цифра спектральної компоненти шуму і в неї починають «вкраплювати» таємне повідомлення. Потім береться інша спектральна компонента шуму і так далі, поки не «вкрапимо» все повідомлення. Стеганоключем при цьому буде номер останньої вірної цифри і номери спектральних компонент шуму, куди ми «вкрапили» таємне повідомлення. Стеганоключ треба передати одержувачу таємного повідомлення по таємному каналу зв'язку.

Тепер щодо стійкості такого стеганолгоритму. Безумовно, «вкраплюючи» таємне повідомлення, ми збурюємо наш контейнер (обернене ШПФ від спектрального стеганоконтейнера). Але величина цього збурення буде на рівні похибки заокруглення стеганоалгоритму і стеганоаналітик не зможе дослідити – чи це контейнер, чи стеганоконтейнер. В цьому полягає стійкість стеганоалгоритму. За визначенням, якщо нам вдається приховати таємну інформацію в шуми контейнера, то ми вже маємо стійкий стеганоалгоритм. У нашому випадку ми пішли далі – нам вдалося не тільки приховати таємну інформацію в спектральні компоненти шуму, а і зробити це з похибкою, яка зіставлювана із похибкою заокруглення стеганоалгоритму.

Завершимо тим, що визначення номеру останньої правильної цифри залежить від якості оцінок заокруглення [10]. Чим точніші оцінки, тим менше збурення ми внесемо в стеганоконтейнер і тим краще буде стійкість стеганоалгоритму.

Висновки. Врахування похибки заокруглення – важливий фактор при оцінці точності наближеного розв'язання задач складності вище середньої.

Список літератури

1. Иванов В.В. Методы вычисления на ЭВМ: Справочное пособие. Киев: Наук. думка, 1986. 584 с.
2. Воеводин В.В. Ошибки округления и устойчивость в прямых методах линейной алгебры. М.: ВЦ МГУ, 1969. 154 с.
3. Уилкинсон Дж.Х. Алгебраическая проблема собственных чисел. М.: Наука, 1970. 564 с.
4. Ramos G.U. Roundoff error analysis of the fast Fourier transform. *Mathematics of Computation*. 1971. **25** (116). 757–768. https://www.ams.org/journals/mcom/1971-25-116/S0025-5718-1971-0300488-0/S0025-5718-1971-0300488-0.pdf
5. Weinstein C.J. Roundoff noise in floating point fast Fourier transform computation. *IEEE Trans. Audio and Electroaconst*. 1969. **19** (2). P. 209–215.
6. Задірака В.К., Олексюк О.С. Комп'ютерна арифметика багаторозрядних чисел. Наукове видання. К.: 2003. 264 с.
7. Задірака В.К., Мельникова С.С., Терещенко А.М. Про асимптотичну ефективність алгоритму Шенхаге-Штрассена. Праці міжнар. конф. *«Питання оптимізації обчислень (ПОО-XXXII)»*, присвяч. 75-річчю від дня народження академіка В.С. Михалевича. К.: Ін-т кібернетики ім. В.М. Глушкова НАН України, 2005. С. 82–83.

8. Задірака В.К., Терещенко А.М. Комп’ютерна арифметика багаторозрядних чисел у послідовній та паралельній моделях обчислень. К.: Наук. думка, 2021. 136 с.
9. Задірака В.К., Мельнікова С.С., Бородавка Н.В. Спектральні алгоритми комп’ютерної стеганографії. *Искусственный интеллект*. 2002. 3. С. 532–541. http://iai.dn.ua/public/JournalAI_2002_3/Razdel4/11_Zadiraka_spektralni.pdf
10. 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. 12. С. 101–112. http://dspace.nbuv.gov.ua/bitstream/handle/123456789/133865/10-Zadiraka.pdf?sequence=1

Одержано 22.06.2021

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

UDC 519.65

Valerii Zadiraka, Inna Shvidchenko *

Using Rounding Errors in Modern Computer Technologies

V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine, Kyiv
* *Correspondence: inetsheva@gmail.com*

Introduction. When solving problems of transcomputational complexity, the problem of evaluating the rounding error is relevant, since it can be dominant in evaluating the accuracy of solving the problem.

The ways to reduce it are important, as are the reserves for optimizing the algorithms for solving the problem in terms of accuracy. In this case, you need to take into account the rounding-off rules and calculation modes.

The article shows how the estimates of the rounding error can be used in modern computer technologies for solving problems of computational, applied mathematics, as well as information security.

The purpose of the article is to draw the attention of the specialists in computational and applied mathematics to the need to take into account the rounding error when analyzing the quality of the approximate solution of problems. This is important for mathematical modeling problems, problems using Bigdata, digital signal and image processing, cybersecurity, and many others.

The article demonstrates specific estimates of the rounding error for solving a number of problems: estimating the mathematical expectation, calculating the discrete Fourier transform, using multi-digit arithmetic and using the estimates of the rounding error in algorithms for solving computer steganography problems.

The results. The estimates of the rounding error of the algorithms for solving the above-mentioned classes of problems are given for different rounding-off rules and for different calculation modes.

For the problem of constructing computer steganography, the use of the estimates of the rounding error in computer technologies for solving problems of hidden information transfer is shown.

Conclusions. Taking into account the rounding error is an important factor in assessing the accuracy of the approximate solution of problems of the complexity above average.

Keywords: rounding error, computer technology, discrete Fourier transform, multi-digit arithmetic, computer steganography.