УДК 519.9
DOI: 10.32626/2308-5878.2019-19.142-148

І. В. Сергієнко, д-р фіз.-мат. наук, професор,
В. К. Задірака, д-р фіз.-мат. наук, професор,
І. В. Швідченко, канд. фіз.-мат. наук

Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ

ВІД ТЕОРІЇ ПОХИБОК ДО СУЧАСНИХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

Робота підводить підсумок розвитку обчислювальної математики за 50 років (1969–2019 рр.) в галузі точності та ефективності обчислювальних алгоритмів.

Зокрема, наголошено на повній похибці обчислювального алгоритму (о. а.), оцінках її якості, постановці задач оптимізації обчислень, оптимальних за точністю та швидкодією о. а., резервах оптимізації обчислень, тестуванні якості прикладного програмного забезпечення, комп'ютерних технологіях розв'язання задач прикладної та обчислювальної математики з заданими значеннями характеристик якості за точністю та швидкодією.

Ключові слова: *теорія обчислень, теорія похибок, апріорна інформація, оптимальні алгоритми, комп'ютерні технології.*

Вступ. У шістдесяті роки минулого сторіччя був бурхливий розвиток обчислювальної математики. Було створено багато методів розв'язання типових класів задач обчислювальної математики: систем лінійних та нелінійних рівнянь, відновлення функцій і функціоналів, задачі Коші для систем диференційних рівнянь, інтегральних та сингулярних рівнянь, математичної фізики, мінімізації функцій і функціоналів, прикладної статистики тощо.

Немає таких методів, які були б завжди кращими за інші. Кожен метод має диференційовану поведінку і є кращим за інші при параметрах о. а. з певної області. На той час ця важлива теза не всіма усвідомлювалась і тому кожний з авторів того чи іншого методу відстоював (часом безпідставно) його якість. Часом на наукових семінарах та захистах дисертацій доходило до бійок.

Чому це було так? Не було чітких критеріїв якості о. а. Це з одного боку. А з іншого — не було оцінок знизу похибки розв'язку задачі (які, до речі, не залежать від о. а., а лише від задачі), не враховувались інші джерела похибок, які реально супроводжують обчислювальний процес, інші характеристики о. а. (обчислювальні ресурси, необхідні для розв'язання задачі) та інше.

Така була реальна ситуація. Тому питання точності й ефективності о. а. були і є досить актуальними [1].

У статті розглядаються шляхи розв'язання цих проблем, методи побудови (при даній інформації про задачу) оптимальних за точністю або швидкодією о. а., застосування теорії похибок, загальної теорії оптимальних алгоритмів, теорії тестування якості прикладного програмного забезпечення для створення сучасних комп'ютерних технологій розв'язання задач прикладної та обчислювальної математики з заданими значеннями характеристик якості за точністю та швидкодією.

Математичні школи, які працюють у цьому напрямку зосереджені в Каліфорнійському, Московському, Варшавському університетах та в інститутах кібернетики та математики НАН України.

1. Комплексний підхід до оцінки якості наближеного розв'язку задач. В шістдесяті роки минулого сторіччя працювали різні математичні школи. Одні з них вивчали похибки метода при розв'язанні тих чи інших задач, інші досліджували неусувну похибку і пропонували методи розв'язання некоректних задач; оцінювали похибку заокруглення алгоритмів. Але кожна з цих шкіл досліджувала лише один вид похибок: метода, неусувної та заокруглення. А в реальній ситуації присутні всі три види похибок. Неврахування хоча б однієї з них на практиці не дає гарантії якості наближеного розв'язку задачі. Наприклад, неврахування похибки заокруглення може призвести до того, що комп'ютерні моделі не мають нічого спільного з фізичними моделями.

Тому на першому Симпозіумі і літній математичній школі 1969 року основна увага була приділена оцінкам повної похибки о. а. для деяких типових класів задач обчислювальної математики. Інтерес до цієї тематики був дуже великий. Про це свідчить кількість учасників Симпозіуму — 462.

Оцінка абсолютної похибки $E(I, X, Y)$ о. а. має вигляд

$$E(I, X, Y) \le \Delta_H(I, X, Y) + \Delta_M(I, X, Y) + \Delta_3(I, X, Y), \qquad (1)$$

де $\Delta_H(I, X, Y)$ — неусувна похибка о. а., $\Delta_M(I, X, Y)$ — похибка методу; $\Delta_3(I, X, Y)$ — похибка заокруглення о. а., I, X, Y — скінченні множини параметрів від яких суттєво залежать задача, о. а. та комп'ютер.

Особливо важливими є питання якості оцінок E та її складових. З позицій обчислювальної математики непокращувані оцінки не завжди нас влаштовують, оскільки вони досягаються на екзотичних задачах, які на практиці, як правило, не зустрічаються. Іноді нас більше влаштовують статистичні оцінки, які більше орієнтовані на реальні задачі [2].

2. Інші характеристики о. а. Окрім характеристики точності $E(I, X, Y)$ в практиці чисельного розв'язання задач за допомого сучасних комп'ютерів розглядають і інші характеристики о. а., які будемо ототожнювати з програмою на комп'ютері.

Нехай задачі $P(I)$ розв'язуються о. а. $A(X)$ на комп'ютері $C(Y)$. Важливе значення (для порівняльного аналізу о. а. та в загальних постановках задач оптимізації обчислень) мають наступні характеристики задач, о. а. та комп'ютерів:

- $T(I,X,Y)$ — час, необхідний для розв'язання задачі $P(I)$ о. а. $A(X)$ на комп'ютері $C(Y)$;
- $M(I,X,Y)$ — необхідна для цього пам'ять комп'ютера.

Відомо, що час T вбирає у себе наступні види робіт: введення та виведення даних T_1; обчислення розв'язку задачі T_2; обмін з зовнішніми накопичувачами T_3; додаткові обчислення T_4 (наприклад, вибір параметрів алгоритму); обчислення оцінок характеристик та інші.

Оскільки деякі з перерахованих робіт можуть виконуватись одночасно, то

$$T \le T_1 + T_2 + T_3 + T_4.$$

Оцінка пам'яті M, необхідної для розв'язання задачі, обчислюється за формулою

$$M \le \sum_{i=1}^{n} k_i N_i + \sum_{j=1}^{m} MF_j + MP,$$

де n — кількість масивів різної розмірності N_i, які використовуються в програмі розв'язання задачі, k_i — число масивів розмірності N_i; m — кількість програмних модулів, які мають бути написані користувачем для розв'язання його задачі; MF_j — оцінка пам'яті, для написаного користувачем модуля; MP — частина оцінки пам'яті (для даного транслятора) для розміщення самої програми. Наведені характеристики о. а., безумовно, не є єдино можливими.

3. Постановка задачі оптимізації обчислень. Оптимізація обчислень полягає в оптимізації однієї з введених характеристик (в загальному випадку по I,X,Y) при дотриманні обмежень на інші характеристики.

Наведемо дві основні постановки задач [2].

Мінімізація часу $T(I,X,Y)$ при дотриманні реальних (Re) обмежень на E і M:

$$T(I,X,Y) = \min_{I,X,Y};$$

$$E(I,X,Y) \le E_{\mathrm{Re}};\ \ M(I,X,Y) \le M_{\mathrm{Re}}.$$

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

$$E(I, X, Y) = \min_{I,X,Y};$$

$$T(I, X, Y) \le T_{\text{Re}}; \;\; M(I, X, Y) \le M_{\text{Re}}.$$

Можливі й імовірнісні постановки задач оптимізації обчислень [3].

4. Оптимальні за точністю та швидкодією обчислювальні алгоритми. Ця тематика широким фронтом почала розвиватись після робіт М. С. Бахвалова [4] (роботи С. М. Нікольського у 1958 р. присвячені лише чисельному інтегруванню) та В. В. Іванова [5]. З 1971 року ця тематика опанувала наукові форуми «Питання оптимізації обчислень». Монографія [6] з'явилась лише у 1983 році.

Одним з основних критеріїв оптимальності о. а. може слугувати вимога його максимальної точності при наявній інформації про задачу і заданих обчислювальних ресурсах. При цьому вважається, що вихідна інформація задана наближено і застосовуються різні стратегії прийняття рішень (визначення оптимального о. а.): чиста (чебишовський центр області невизначеності розв'язків задачі, метод нев'язки, квазіоптимальний метод), послідовна [4, 7], послідовно-оптимальна [8].

В рамках чистої стратегії частіше всього використовується метод «капелюхів» М. С. Бахвалова та метод граничних функцій (МГФ), розроблений в Інституті кібернетики АН УРСР [7]. МГФ щільно застосовується в умовах найбільш повного використання апріорної інформації про задачу. Там, де її не вистачає, використовуються алгоритми її виявлення [9]. Це дає змогу зменшити похибку оптимального алгоритму на більш вузькому класі задач, який генерується цією додатковою апріорною інформацією [10].

Оптимальні за швидкодією о. а. потрібні в першу чергу для задач, які потребують розв'язання в режимі реального часу або для розв'язання задач трансобчислювальної складності, задач крипто та стеганоаналізу [11]. Багато оптимальних за швидкодією алгоритмів використовують швидкі ортогональні перетворення [2].

5. Тестування якості прикладного програмного забезпечення. Задача розробки якісного програмного забезпечення є найбільш важливою у загальній проблемі створення обчислювальних систем. Тому дослідження питань, пов'язаних з розробкою принципів і методів створення якісного програмного забезпечення, є досить важливим. Перш за все це стосується прикладних програм, призначених для розв'язання типових класів задач обчислювальної математики.

Експериментальні дослідження о. а. полягають у проведенні за різними критеріями числових обчислювальних експериментів (тестування) за допомогою наборів спеціально розроблених задач (тестів) для визначення функціональних можливостей о. а., кількісних показників їх характеристик і областей їх диференційованої поведінки за

цими характеристиками, порівняння програм за різними критеріями якості тощо [12]. Запропонований метод тестування базується на концепції поєднання теоретичних досліджень чисельних методів і о. а., враховуючи теорію оцінок похибок, що супроводжують обчислювальний процес, і експериментальних досліджень.

6. Резерви оптимізації обчислень. На наукових форумах розглядались наступні резерви поліпшення характеристик якості розв'язку задачі та обчислювального процесу [13].

Резерви зменшення похибок:

- за рахунок неточності вхідних даних:
  - уточнення класу задач;
  - підвищення точності вхідної інформації.
- методу:
  - використання оптимальних о. а.;
  - перехід в інший клас інформаційних операторів;
  - повне використання вхідної інформації для звуження класу задач;
- заокруглень:
  - використання схем обчислень, що мінімізують швидкість накопичення похибки заокруглень;
  - збільшення довжини розрядної сітки;
  - вибір та моделювання правила заокруглення.

Резерви зменшення процесорного часу:

- поліпшення точності оцінок похибок методу та заокруглень;
- узгодження о. а. з архітектурою комп'ютера;
- використання «швидкої» арифметики [14];
- розпаралелювання обчислень;
- спеціалізовані обчислювачі.

7. Елементи комп'ютерної технології (КТ) розв'язання задач із заданими значеннями характеристик якості. КТ як загального плану, так і для конкретних класів задач, доповідались на наукових форумах «Питання оптимізації обчислень» з 2000 року [15].

Побудова наближеного ε — розв'язку задачі $P \in \mathrm{P}$ при обмежених обчислювальних ресурсах може бути описана умовами:

$$E(I, X, Y) \le \varepsilon, \tag{2}$$

$$T(I, X, Y, \varepsilon) \le T_0(\varepsilon), \tag{3}$$

$$M(I, X, Y, \varepsilon) \le M_0(\varepsilon), \tag{4}$$

де ε, T_0, M_0 — задані числа.

Концепція КТ полягає у наступному:

- задаються ε, $T_0(\varepsilon)$, $M_0(\varepsilon)$;

- з деякої множини о. а. і програм знаходиться (або розробляється) о. а. і програма, яка може забезпечити якість (2)–(4);
- за допомогою розробленої або наявної програми обчислюється розв'язок задачі із заданими значеннями характеристик якості.

КТ щільно використовує теорію похибок і перелічені вище резерви оптимізації обчислень.

Висновки. Викладені деякі віхи розвитку теорії обчислень, які щільно обговорювались і докладались на міжнародних наукових форумах «Питання оптимізації обчислень» вподовж 1969–2018 років.

Список використаних джерел:

1. Иванов В. В. Вопросы точности и эффективности вычислительных алгоритмов. Киев : Ин-т кибернетики АН УССР, 1969. 135 с.
2. Задирака В. К. Теория вычисления преобразования Фурье. Киев : Наук. думка, 1983. 216 с.
3. Кендалл М. Дж., Стюарт А. Статистические выводы и связи. М. : Наука, 1973. 899 с.
4. Бахвалов Н. С. О свойствах оптимальных методов решения задач математической физики. *Журн. вычисл. математики и мат. физики.* 1970. Т. 10, № 3. С. 555–568.
5. Иванов В. В. Об оптимальных алгоритмах минимизации в классах дифференцируемых функций. Докл. АН СССР. 1971. Т. 201, № 3. С. 527–530.
6. Трауб Дж., Вожняковский Х. Общая теория оптимальных алгоритмов. М. : Мир, 1983. 382 с.
7. Иванов В. В., Задирака В. К. Вопросы оптимизации вычислений. К. : О-во «Знание» УССР, 1978. 34 с.
8. Сухарев А. Г. Оптимальный метод построения наилучших равномерных приближений для функций некоторого класса. *Журн. вычисл. математики и мат. физики*. 1978. Т. 18, № 9. С. 302–313.
9. Сергієнко І. В., Задірака В. К., Литвин О. М. Елементи загальної теорії оптимальних алгоритмів та суміжні питання. Киев : Наукова думка, 2012. 400 с.
10. Сергієнко І. В., Задірака В. К., Швідченко І. В. Наукова тематика міжнародних математичних форумів з питань оптимізації обчислень. *Математичне та комп'ютерне моделювання.* Серія: Фізико-математичні науки. 2017. Вип. 15. С. 189–193.
11. Задірака В. К., Кошкіна Н. В., Швідченко І. В. Комп'ютерній стеганографії 20 років. *Матеріали V міжнар. наук.-техн. конф. «Захист інформації і безпека інформаційних систем»* (2–3 червня 2016 р.). Львів, 2016. С. 98–99.
12. Бабич М. Д., Задирака В. К., Сергиенко И. В. Вычислительный эксперимент в проблеме оптимизации вычислений. II. *Кибернетика и системный анализ.* 1999. № 2. С. 59–79.
13. Бабич М. Д., Задирака В. К., Людвиченко В. А., Сергиенко И. В. Об использовании резервов оптимизации вычислений в компьютерных технологиях решения задач прикладной и вычислительной математики с требуемыми значениями характеристик качества. *Журнал вычислительной математики и математической физики.* 2010. Т. 50, № 12. С. 2285–2295.

14. Задірака В. К., Олексюк О. С. Комп'ютерна арифметика багаторозрядних чисел. Київ, 2003. 264 с.
15. Сергиенко И. В., Задирака В. К., Бабич М. Д., Березовский А. И., Бесараб П. Н., Людвиченко В. А. Компьютерные технологии решения задач прикладной и вычислительной математики с заданными значениями характеристик качества. *Кибернетика и системный анализ*. 2006. № 5. С. 33–41.

FROM ERROR THEORY TO MODERN COMPUTER TECHNOLOGIES

The article summarizes the development of computational mathematics during 50 years' period (1969–2019) in the field of accuracy and efficiency of computational algorithms.

In particular, it is emphasized on the global error of the computational algorithm (c. a.), estimates of its quality, the formulation of computations optimization problems, computational algorithms that are optimal in accuracy and processing speed, reserves of calculations optimization, testing the quality of applied software, computer technologies solving the problems of applied and computational mathematics with the given values of quality characteristics in accuracy and processing speed.

Key words: *theory of computing, error theory, apriori information, optimal algorithms, computer technologies.*

Одержано 31.01.2019

УДК 512.7+512.9,688.321
DOI: 10.32626/2308-5878.2019-19.148-155

Р. В. Скуратовский, преподаватель

Межрегиональная академия управления персоналом, г. Киев

РЕШЕНИЕ ОБРАТНОЙ ЗАДАЧИ К УДВОЕНИЮ ТОЧКИ СКРУЧЕННОЙ КРИВОЙ ЭДВАРДСА НАД КОНЕЧНЫМ ПОЛЕМ

Получено решение задачи обратной к удвоению точки для кривой представленной в скрученной форме Эдвардса. Получены оценки сложности операции деления на два в сравнении с удвоением точки. Найдено одно из приложений свойств делимости точки на два для определения порядка точки в криптосистеме основаной на проблеме дискретного логарифма.

Найдены необходимые и достаточные условия делимости точки $G=(X,Y)$ кривой $E_{a,d}$ на 2. Исследовано возможность применения данных кривых для генерации криптостойкой последовательности большого периода. Важность операции делимости точки на 2 при криптоанализе уже частично замечена криптографами.