2. Townsend K. Solving the Quantum Decryption ‘Harvest Now, Decrypt Later’ Problem. URL: https://www.securityweek.com/solving-quantum-decryption-harvest-now-decrypt-later-problem/ (дата звернення: 19.05.2023).

3. Korchenko O., Vasiliu Y., Gnatyuk S. Modern quantum technologies of information security against cyber-terrorist attacks. Aviation. 2010. T. 14, № 2. C. 58–69.

4. Sharma, M. K., & Nene, M. J. (2020). Quantum one time password with biometrics. In Innovative Data Communication Technologies and Application: ICIDCA 2019 (pp. 312-318). Springer International Publishing.

УДК 612:656.7.086.1 (044)

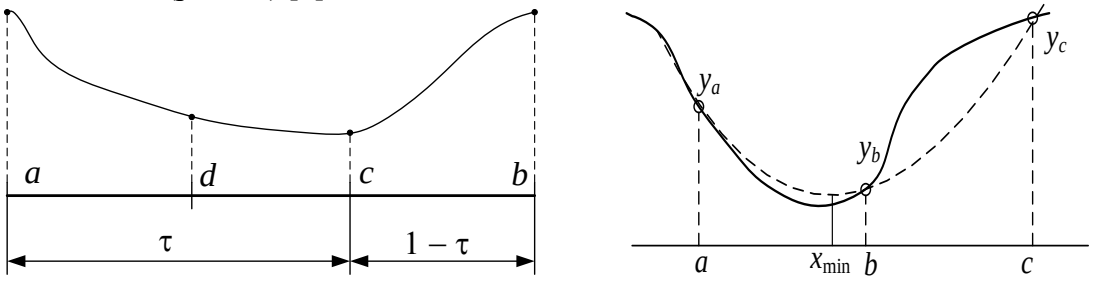
Бориченко М.Ю., канд. техн. наук, доцент
Іванець О.Б., канд. техн. наук, доцент
Архирей М.В.
Корчемний М.С., студент
Шевченко Т.Р., студентка
Національний авіаційний університет, м. Київ, olchik2104@ukr.net

ОПТИМІЗАЦІЯ ФУНКЦІЙ НА ОСНОВІ МЕТОДІВ ВСТАНОВЛЕННЯ ІНТЕРВАЛІВ НЕВИЗНАЧЕНОСТІ

Складнощі аналізу складних об’єктів полягає в наявності джерел невизначеності первинної інформації про параметри даних об’єктів [1,2]. Для побудови алгоритмів одновимірної оптимізації цільової функції використовують методи встановлення інтервалу невизначеності [3].

В роботі проаналізоване використання наступних методів оптимізації для зменшення інтервалів невизначеності при аналізі складних об’єктів різної природи: метод золотого перерізу, метод параболічної інтерполяції, метод Брента [4].

Метод золотого перерізу, що полягає у використанні золотого перерізу відрізка за рахунок ділення відрізка на дві частини, при якому відношення довжини всього відрізка до довжини більшої частини дорівнює відношенню довжини більшої частини до довжині меншої частини (рис. 1а) [3].



а) б)

Рис. 1 – Графічне представлення методів оптимізації: а)метод золотого перерізу, б) метод параболічної інтерполяції

Після кожній ітерації алгоритму довжина поточного інтервалу невизначеності $L = b – a$ скорочується в τ разів. Кількість ітерацій K, необхідних для знаходження мінімуму функції $f(x)$ з точністю ε, можна оцінити з умови $(b – a)\tau^K \le \varepsilon$.

Метод параболічної інтерполяції застосовує поліном низького порядку $P(x)$ для апроксимації цільової функції на інтервалі пошуку, а потім використовують точку мінімуму полінома апроксимації P(x) як точку ділення нового інтервалу, причому якщо функція поблизу мінімуму близька до параболічної, то парабола проведена через три точки цієї функції може одним кроком привести до мінімуму, або дуже близько до нього.

В якості точки мінімуму функції *f(x)* приймають аналітично обчислену точку мінімуму зазначеної параболи. Метод має суперлінійну швидкість збіжності, проте лише в малій околиці точки мінімуму xmin. Метод не використовує оцінки похідних цільової функції, тому ефективний для функцій, що складно диференціювати. На початкових кроках процесу оптимізації метод може стати чисельно нестійким [5].

Метод Брента поєднує повільний але надійний метод золотого перерізу з більш швидким методом зворотної параболічної інтерполяції, якій в свою чергу може виявитися не досить надійним. Метод Брента використовує два зазначених методи залежно від поведінки цільової функції на інтервалі пошуку, причому спочатку застосовується параболічна інтерполяція; якщо не отримані прийнятні результати, то застосовується пошук золотого перерізу, щоб вирішити завдання [6].

Для збіжності методу параболічний крок має: а) знаходитись всередині обмеженого інтервалу [a, b]; б) передбачати рух від поточного кращого x значення, яке менше, ніж половина руху на передостанньому кроці. В такому разі параболічні кроки сходяться до розв'язку, а не стрибають в деякому граничному циклі.

Особливістю описаних вище методів є їхня ефективність і універсальність. Під ефективністю методів (або їх алгоритмів) розуміють число обчислень функції, необхідне для досягнення необхідного звуження інтервалу невизначеності. Як правило, метод золотого перетину, володіє високою ефективністю, найбільш підходять для розв'язку одновимірних унімодальних задач оптимізації [7].

Універсальність алгоритму означає, що його можна легко застосувати для розв'язку самих різноманітних задач. В цьому відношенні метод параболічної інтерполяції ефективний для функцій, що складно диференціювати [8].

Але для підвищення достовірності використання методів оптимізації випадках слід використати декілька різних алгоритмів і подивитись, чи дають вони усі один і той самий оптимум. Звідси витікає важливий висновок, який слід мати на увазі, розв'язуючи задачі оптимізації: не існує універсального алгоритму, який дозволяв би розв'язувати будь-які задачі [9]. Вирішуючи складні задачі оптимізації, слід користуватися різними методами, так як це дозволяє збільшити долю вигідних розв'язків.

Список посилань

1. Shchapov P.F. Dynamic properties of the time series of results of biomedical measurements / P.F. Shchapov, O.B. Ivanets, O.S. Sevryukova // Science-intensive technologies, 2020. № 2 (46), P. 236 - 244.

2. Kucheruk V. Yu. Approach to the criterion evaluation of the degree of deviation from the norm of the state of the object / V. Yu. Kucheruk, P.I. Kulakov, O.B. Ivanets, A.P. Kulakova // Measuring and computing technology in technological processes, 2020. № 2 (66). P.10-15. DOI: 10.31891 / 2219-9365-2020-66-2-

3. Нефьодов Ю.М. Методи оптимізації в прикладах і задачах. / Ю.М. Нефьодов, Т.Ю. Галицька: Навч. посіб. – К.: Кондор, 2015. – 324 с.

4. Кісельова О.М. Чисельні методи оптимізації: навч. посіб. / О.М. Кісельова, А.Є. Шевельова. – Д.: Вид-во ДНУ, 2008. – 208 с.

5. Еременко В.С. Метод обробки результатів вимірювань медичних показників /В.С. Еременко, М.Ю Бурiченко, О.Б.Іванець // Наукоємні технології, 2020. - № 3(47), С. 392 - 398. DOI: 10.18372/2310-5461.47.14937

6. Optimization Toobox User Guide.

7. Kochenderfer M. J. Algorithms for Optimization. /Mykel J. Kochenderfer, Tim A. Wheeler. – The MIT Press. Cambridge, Massachusetts, London, England, 2019. – 521 p.

8. Мовчан А.П. Навчальний посібник: Методи статичної оптимізації. Навч. посіб. / Мовчан А.П., Степанець О.В. — К.: НТУУ «КПІ», 2012. — 138 с.

9. Kuzmin V.M. Mathematical model for decision making system based on three-segmented linear regression / [V.M. Kuzmin, R.V.Khrashchevskyi, M.S.Kulik et al] // Radio Electronics, Computer Science, Control. — 2022. № 3. – P. 38-49.