УДК 330.4;519.8

Л. А. Білий, Р. О. Циганчук

МОДЕЛЮВАННЯ ДИНАМІКИ ЕКОНОМІЧНИХ ПРОЦЕСІВ, ДИСКРЕТНИХ У ЧАСІ

Запропоновано метод визначення різницевих рівнянь, апроксимуючих диференціальні рівняння. Для зменшення кількості різницевих рівнянь при збереженні необхідної точності результатів доцільно використовувати апроксимації, які враховують більшу кількість членів розкладання шуканого рішення в ряд Тейлора. Коефіцієнти таких апроксимацій знаходимо за методом невизначених коефіцієнтів.

Ключові слова: *неперервний час, дискретний час, динамічна модель, диференціальні рівняння, різницеві рівняння, апроксимація.*

Постановка проблеми. Більшість економіко-математичних моделей характеризується статичним підходом до вивчення економіки, коли її стан досліджується в заданий момент часу. Під статичною економічною системою розуміється така система, координати якої на досліджуваному відтинку часу можуть вважатися сталими. Відповідно, при формулюванні статичної економіко-математичної моделі припускається, що всі залежності відносять до одного моменту часу, а система, що моделюється, є незмінною в часі. При цьому ігноруються можливі, а інколи неминучі зміни, оскільки їхнє врахування не вимагається поставленою метою моделювання.

Крім того, припускається, що всі процеси, які протікають у системі, не вимагають для свого аналізу розгортання в часі, оскільки можуть бути достатньо точно охарактеризовані незалежними від часу величинами. Тому в статичній моделі час не вводиться явно. Статичні моделі характеризують економічну систему на будь-якому фіксованому моменті часу. Оскільки статичні моделі у формалізованому вигляді не містять фактора часу, вони завжди простіші від динамічних моделей тих самих економічних систем, які тією чи іншою мірою враховують цей фактор.

Під динамічною системою розуміють будь-яку систему, яка змінюється в часі. Час в економічній динаміці можна розглядати як неперервний або дискретний. Неперервний час зручний для моделювання, оскільки дає змогу використати апарат диференціального числення і диференціальних рівнянь. Дискретний час зручний для розв'язування прикладних задач, оскільки статистичні дані завжди дискретні і належать до конкретних одиниць часу. Для дискретного часу використовують апарат різницевих рівнянь [1].

Математичний опис динамічних моделей здійснюється, як правило:

– системами диференціальних рівнянь, у яких неперервною змінною є час;
– різницевими рівняннями, де час – дискретна величина;
– системами звичайних алгебраїчних рівнянь.

За допомогою динамічних моделей, зокрема, розв'язують задачі планування і прогнозування економічних процесів [2]:

– визначення траєкторії розвитку економічної системи та її стан у задачі в моменти часу;
– аналіз економічної системи на стійкість;
– аналіз структурних зсувів.

У практичній діяльності використовують багатогалузеві динамічні моделі розвитку економіки, виробничі функції, теорія економічного зростання.

Диференціальні рівняння знаходять достатньо широке застосування в моделях динамічної економіки, в яких відображається не лише залежність змінних від часу, а й їхній взаємозв'язок у часі.

Аналіз динамічних систем і їхнє математичне моделювання базуються на чисельних методах розв'язування систем диференціальних рівнянь. Особливе місце серед чисельних методів розв'язування динамічних моделей із дискретним часом займає метод скінченних різниць [3]. Універсальність, можливість застосування в лінійних і нелінійних задачах роблять метод скінченних різниць найпоширенішим методом із застосовуваних у даний час наближених методів. Але не лише надзвичайна загальність різницевого методу приваблює дослідників. Мабуть, це найбільш зручний і прозорий чисельний метод, завдяки якому майже завжди можна отримати уявлення про шуканий розв'язок.

Передати ідею методу скінченних різниць можна буквально в кількох словах. Уявіть собі, що перед вами – задача про знаходження наближеного розв'язку деякого диференціального рівняння

$$\frac{dx}{dt} = f(x,t) \tag{1}$$

за початкових умов

$$x(t_0) = x_0. \tag{2}$$

Якщо початкові умови (2) задають в одній точці t_0, то сукупність звичайного диференціального рівняння і початкової умови називають задачею Коші [4].

Виникає питання: чи не можна спростити задане рівняння, позбавившись якимось чином від похідної шуканої функції $f(x, t)$?

Найпростіший шлях розв'язання цієї задачі міститься у визначенні похідної

$$\frac{dx}{dt} = \lim_{\Delta t \to 0} \frac{f(x + \Delta x, t) - f(x, t)}{\Delta t}. \tag{3}$$

Дійсно, якщо відкинути в цій рівності знак границі, то отримаємо наближену формулу

$$\frac{dx}{dt} \approx \frac{f(x + \Delta x, t) - f(x, t)}{\Delta t}, \tag{4}$$

яка дає змогу замінити похідну dx/dt різницевим відношенням, розміщеним у правій частині формули (4). Похідні більш високого порядку також можуть бути апроксимовані різницевими відношеннями подібного вигляду.

Таким чином, якщо всі похідні шуканої функції $f(x, t)$, які входять у диференціальне рівняння, замінити відповідними різницевими відношеннями, що апроксимують ці похідні, то отримаємо різницеве рівняння, яке в математичному сенсі буде задачею, більш простою від задачі Коші. Розв'язок $F(x, t)$ отриманого різницевого рівняння, що є апроксимацією диференціального рівняння, вважають наближеним розв'язком диференціального рівняння.

У кінцево-різницевому рівнянні, яке апроксимує диференціальне, x і t є неперервні змінні, тому саме це рівняння і називається рівнянням із неперервними аргументами. Розв'язати таке рівняння важко, а часто і зовсім неможливо. У зв'язку з цим замість кінцево-різницевих рівнянь із неперервними аргументами розглядають відповідні йому різницеві рівняння з дискретними аргументами, коли незалежні змінні x і t отримують дискретну множину значень, наприклад

$$x_i = ih,\ i = 0; \pm 1, \pm 2, \ldots, \tag{5}$$

де $h = \Delta t$.

У результаті диференціальне рівняння замінюємо кінцево-різницевим рівнянням із дискретними аргументами. Легко бачити, що таке різницеве рівняння можна тлумачити як систему лінійних алгебраїчних рівнянь стосовно невідомих x_i, у якій число рівнянь рівне числу невідомих. Розв'язуючи отриману систему алгебраїчних рівнянь, знаходять наближені значення шуканого розв'язку $f(x, t)$. Якщо крім диференціального рівняння була задана початкова умова, то і вона також повинна бути замінена різницевими початковими умовами для функції f_i, які повинні розглядатися разом з отриманою раніше системою алгебраїчних рівнянь.

Мета дослідження. Для зменшення кількості кінцево-різницевих рівнянь, які апроксимують диференціальні рівняння, при збереженні потрібної точності результатів дослідження, необхідно скористатись апроксимаціями, які враховують не лише перший член розкладання шуканого рішення в ряд Тейлора, а й наступні його члени. Коефіцієнти таких апроксимацій можна знайти за методом невизначених коефіцієнтів [5].

Результати дослідження. Для того щоб отримати різницеву схему, яка приблизно описувала б диференціальне рівняння або систему таких рівнянь, треба здійснити два кроки.

1. Замінити область неперервної зміни аргументу областю дискретної його зміни.
2. Замінити диференціальні оператори деякими різницевими операторами, а також сформулювати різницевий аналог для початкових умов.

Після цього задача про чисельне розв'язування вихідного диференціального рівняння або їх системи зводиться до питання знаходження рішення отриманої алгебраїчної системи.

При чисельному розв'язуванні задачі ми, очевидно, не можемо відтворити різницеве рішення для всіх значень аргументу, змінного в деякій області евклідового простору. Природно тому вибрати в цій області деяку кінцеву множину точок і наближені розв'язки шукати лише в цих точках. Така множина точок називається сіткою. Окремі точки називаються вузлами сітки.

Функція, визначена у вузлах сітки, називається сітковою функцією. Таким чином, ми замінимо область неперервної зміни аргументу сіткою, тобто областю дискретної зміни аргументу, інакше кажучи, ми здійснюємо апроксимацію простору рішень диференціальних рівнянь простором сіткових функцій.

Апроксимація диференціальних рівнянь кінцево-різницевими пов'язана з певними труднощами, основні ось які.

1. Вибір кроку апроксимацій – відстані між сусідніми вузлами, який диктується такими міркуваннями. По-перше, ураховується характер шуканого рішення: плавна зміна функції дає змогу взяти більший крок. По-друге, враховується точність, з якою шукається розв'язок задачі. Вища точність вимагає дрібнішого кроку.
2. Вибір різницевого виразу як аналога диференціальних рівнянь. Існує очевидне протиріччя: збільшення числа вузлів у різницевому виразі підвищує точність розв'язку, але в той же час призводить до ускладнення методу.
3. Чи існує розв'язок системи різницевих рівнянь?
4. Чи зійдеться рішення системи різницевих рівнянь до рішення диференціальної задачі при зменшенні кроку?
5. Яка похибка різницевого рішення, тобто наскільки точний розв'язок системи різницевих рівнянь відрізняється від точного розв'язку диференціальних рівнянь?
6. Який найкращий спосіб розв'язування системи різницевих рівнянь?

Усі ці питання є предметом інтенсивних досліджень математиків-прикладників.

Основні результати теорії і різноманітну бібліографію наведено в монографіях [6; 7].

Наша робота присвячена розробленню методу побудови різницевих апроксимацій, які враховують вищі члени розкладу шуканих функцій у ряд Тейлора.

Приклад найпростішої різницевої апроксимації подано виразом (4). У випадку диференціальних рівнянь зі змінними коефіцієнтами задача побудови різницевих схем суттєво ускладнюється. Для заданої дискретизації часу можна побудувати безліч схем, еквівалентних за порядком апроксимації. Безумовно, дослідникові бажано мати схему з можливо більш високим порядком точності. Практично це означає, що треба шукати схеми з мінімальною кількістю точок дискретизації за максимально можливого на цій сітці порядку апроксимації.

Найбільш загальний спосіб побудови кінцево-різницевих рівнянь полягає в тому, що відповідним різницевим відношенням апроксимується не кожна похідна зокрема, а відразу весь диференціальний оператор $L(x)$. При цьому кількість вибраних вузлів дискретизації не може бути меншою від певного числа. Мінімальний набір вузлів визначається перш за все порядком даного диференціального рівняння. За заданого набору вузлів складають кінцево-різницеве рівняння, яке апроксимує дане диференціальне рівняння в m-й вузловій точці, яка лежить посередині сукупності вузлів із номерами $m-k, ..., m, ..., m+k (k=1, 2, ...)$ і яке записуємо так:

$$a_{m-k}Y_{m-k} + ... + a_m Y_m + ... + a_{m+k}Y_{m+k} = h(b_{m-k}Y'_{m-k} + ... + b_m Y'_m + ... + b_{m+k}Y'_{m+k}) + R_k. \quad (6)$$

Число k називається порядком цього рівняння, а число p – його степенем. Залишковий член R_k означає різницю між лівою і правою частинами виразу (6) і визначає помилку апроксимації.

Розкладаємо точкові функції $Y_{m-k}, ..., Y_m, ..., Y_{m+k}$ та їхні похідні $Y'_{m-k}, ..., Y'_m, ..., Y'_{m+k}$ за формулою Тейлора до членів із похідними степеня p + 1. Отримаємо

$$Y_{m+k} = Y_m + khY'_m + \frac{(kh)^2}{2!}Y''_m + ... + \frac{(kh)^p}{p!}Y^p_m + \frac{(kh)^{p+1}}{(p+1)!}Y^{p+1}_m + 0(h^{p+1}), \quad (7а)$$

$$Y'_{m+k} = Y'_m + khY''_m + \frac{(kh)^2}{2!}Y''_m + ... + \frac{(kh)^{p-1}}{(p-1)!}Y^p_m + \frac{(kh)^p}{p!}Y^{p+1}_m + 0(h^p). \quad (7б)$$

Поставимо вимогу, щоб після підстановки (7а) і (7б) у (6) коефіцієнти при похідних у правій частині виразу (6) збіглися з коефіцієнтами при відповідних похідних лівої частини. У результаті отримаємо систему алгебраїчних рівнянь

$$\sum_{0}^{K} a_K = 0, \tag{8а}$$

$$\sum_{1}^{K} a_K K^S - S b_K K^{S-1}) = 0,\ (S = 2, 3, ..., p),\ \sum_{1}^{K} a_K K - \sum_{0}^{K} b_K = 0. \tag{8б}$$

Усього маємо $p + 1$ однорідних лінійних алгебраїчних рівнянь відносно $2(K + 1)$ невідомих $a_{m\pm K}$, $b_{m\pm K}$. Якщо ця система рівнянь має рішення, то задача побудови кінцево-різницевого рівняння, апроксимуючого задане диференціальне, може вважатися розв'язаною.

Знайдемо за методом невизначених коефіцієнтів значення коефіцієнтів a і b для рівнянь різного порядку K.

Візьмімо $K = 1$. Тоді рівняння (8) будуть такі:

$$\begin{aligned} & a_{m-1} + a_{m+1} + a_m = 0; \\ & -a_{m-1} + a_{m+1} = h \times 1(b_{m-1} + b_{m+1} + b_m); \\ & a_{m-1} + a_{m+1} = h \times 2(-b_{m-1} + b_{m+1}); \\ & -a_{m-1} + a_{m+1} = h \times 3(b_{m-1} + b_{m+1}). \end{aligned} \tag{9}$$

Враховуючи, що для заданої дискретизації аргументу можна побудувати безліч різницевих схем, еквівалентних за порядком апроксимації, і не впливаючи на загальність результату в системі рівнянь (9) приймімо $a_m = 1$, $b_m = 0$. Результатом розв'язування буде формула

$$2y_{m-1} - 4y_m + 2y_{m+1} = h(y'_{m-1} + y'_{m+1}) + \frac{1}{24} h^4 y_m^4. \tag{10}$$

Похибка апроксимації різницевим рівнянням (10) функцій, що мають обмежені похідні до п'ятого порядку включно, становить $0(h)^4$.

Якщо в системі рівнянь (9) покласти $a_m = 0$, $b_m = h$, що також ніяк не відіб'ється на загальності отримуваного апроксимуючого виразу, то отримаємо формулу, яка пов'язує між собою функцію та її похідні з похибкою апроксимації $0(h)^5$.

Різницеве рівняння для $K = 1$ за умови $a_m = 0$, $b_m = h$ із похибкою п'ятого порядку, отримане в результаті розв'язування системи (9), буде таким:

$$-3y_{m-1} + 3y_{m+1} = h(y'_{m-1} + 4y'_m + y'_{m+1}) + \frac{1}{30} h^5 y_m^5. \tag{11}$$

Збільшення порядку різницевого рівняння K на кожну одиницю веде до підвищення точності по кроку h на чотири порядки. Крім цього, знаменник у залишковому члені R_K швидко зростає.

Як уже зазначалось, у нашій роботі основна увага зосереджена на алгоритмічному аспекті методу – питанні побудови різницевих рівнянь. Теоретичне доведення збіжності різницевої схеми являє собою складну самостійну наукову проблему. На практиці для доведення збіжності різницевої схеми часто використовують такий прийом. Проводять кілька розрахунків задачі, послідовно зменшуючи крок, тобто збільшуючи число вузлів сітки. На підставі поведінки рішень, отриманих таким способом, судять про збіжність схеми, про порядок її точності.

Висновки

1. Розроблено раціональний спосіб апроксимації диференціальних рівнянь кінцево-різницевими. Отримано різницеві рівняння підвищеної точності, які дають змогу ціною незначного ускладнення розрахункових формул значно скоротити загальне число прораховуваних вузлів, що в кінцевому підсумку призводить до зменшення загального обсягу обчислень.
2. Розв'язування отриманих різницевих рівнянь підвищеної точності стосовно вузлових функцій значно спростять і полегшать процедуру апроксимації диференціальних рівнянь різницевими.

Список використаних джерел

1. Замков О. О., Толстопятенко А. В., Черемных Ю. Н. Математические методы в экономике: Учебник / Под общ. ред. д-ра экон. наук, проф. А. В. Сидоровича; МГУ им. М. В. Ломоносова. – 3-е изд. перероcб. – М.: Изд. «Дело и Сервис», 2004. – 268 с.
2. Шелобаев С. И. Математические методы и модели в экономике, финансах, бизнесе: Учеб. пособие для вузов. – М.: ЮНИТИ ДАНА, 2010. – 367 с.
3. Березин И. С., Жидков Н. П. Методы вычислений. – М.: Физматгиз, 1996. – Т. 2. – 639 с.
4. Фельдман Л. П., Петренко А. І., Дмитрієва О. А. Чисельні методи в інформатиці. – К.: Видавнича група BHV, 2006. – 480 с.
5. Демидович Б. П., Марон И. А. Основы вычеслительной математики / Главная редак. физ.-мат. литературы. – М.: Изд. «НАУКА», 1970. – 660 с.
6. Вазов В., Форсайт Д. Разностные методы решения дифференциальных уравнений в частных производных. – М.: Изд-во иностр. лит., 1963. – 486 с.
7. Самафский А. А. Введение в теорию разностных схем. – М.: Наука, 1971. – 552 с.

Билый Л. А., Цыганчук Р. О.

Моделирование динамики экономических процессов дискретных во времени

Предложен метод определения разностных уравнений, аппроксимирующих дифференциальные уравнения. Для уменьшения количества разностных уравнений при сохранении необходимой точности результатов целесообразно использовать аппроксимации, которые учитывают большее количество членов разложения искомого решения в ряд Тейлора. Коэффициенты таких аппроксимаций находятся методом неопределенных коэффициентов.

Ключевые слова: *непрерывное время, дискретное время, динамическая модель, дифференциальные уравнения, разностные уравнения, аппроксимация.*

Bilyy L. A., Tsyhanchuk R. O.

The method of determination of difference equations approximating differential equations. To reduce the amount of difference equations while maintaining the desired accuracy of the approximation is appropriate, taking into account the large number of members of the decomposition of the desired solution in a Taylor series. Factors such approximations are the method of undetermined coefficients.

Key words: *continuous time, discrete time, dynamic model, differential equations, difference equations, approximation.*

Білий Леонід Адамович – професор, доктор технічних наук, професор кафедри економічної кібернетики Львівського інституту банківської справи Університету банківської справи Національного банку України (м. Київ);

Циганчук Роман Олегович – завідувач редакційного сектору видавництва Університету банківської справи Національного банку України (м. Київ).

УДК 004.056.57:656.2

О. А. Нємкова

RS-АНАЛІЗ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ СИСТЕМ ПОТОКОВОГО ШИФРУВАННЯ

Застосовано RS-аналіз до деяких генераторів псевдовипадкових послідовностей і розраховано значення коефіцієнта Хьорста. Установлена відповідність результатів аналізу до статистичних властивостей генераторів. Запропоновано використовувати RS-аналіз для тестування генераторів псевдовипадкових послідовностей на наявність персистентності, іншими словами – перевіряти генератори на придатність для застосування у криптографії.

Ключові слова: *генератор псевдовипадкової послідовності, коефіцієнт Хьорста, потокове шифрування, лінійний конгруентний генератор, персистентність.*

Постановка проблеми. Відкритість сучасних інформаційних систем, у яких відбувається обробка, збереження та передавання таємної інформації, потребує застосування криптографічних перетворень великих масивів даних. Якість криптографічного перетворення повинна бути дуже високою, тому що переважно це стосується передавання та зберігання банківської інформації, закритих баз даних мобільних операторів, медичних і фармацевтичних компаній, військових розробок та інших даних, що пов'язані з державною