формулі немає. Те, що $V(d)$ є іманентним, слідує з принципу об'єднання, бо інакше він утворився б на передостанньому кроці, а на останньому мали б весь простір *V*. Тому, якщо не існував $V(d),\ d > n/2$, то не утворився б і підпростір $V(a)$, де $a = c + d > 3n/4$, – це слідує з порядку об'єднання – від найменших до більших розмірностей. Тому $(c+d)^3 + 3(c^3 + b^3) < n^3 + 3(n/4)^3 + 3(n/2)^3 \le 2n^3$. У випадку $a = c + d$ підпростір $V(a)$ утворено на останньому кроці, але при цьому $V(d),\ d > n/2$, розташований зкраю. Таким чином маємо оцінку $(c+d)^3 + 3c^3 < n^3 + 3(n/4)^3 < 3n^3$. Лему 4 доведено.

В процесі об'єднання всіх клітин Фробеніуса здійснюємо послідовне додавання їх циклічних векторів і отримуємо циклічний вектор $\vec{c}$ усього арифметичного векторного простору F_p^n. Цей вектор породжує базис Фробеніуса $\vec{c},\ldots,A^{n-1}\vec{c}$, який є в даному випадку нормальним базисом для F_q.

3. Висновок

Запропоновано новий метод побудови нормального базису над скінченним полем, який у класі детермінованих алгоритмів має найкращу побітову оцінку складності $O\left(n^3 \log^2 q\right)$.

1. *Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А.* Элементарное введение в эллиптическую криптографию. – М.: Комкнига, 2006. – Кн. 1. – 321 с. 2. *Боревич З.И., Скопин А.И.* Расширение локального кольца с нормальным базисом для главных единиц // Алгебраическая теория чисел и представления // Тр. МИАН СССР. – М.; Л.: Наука, 1965. – Т. 80. – С. 45–50. 3. *Гантмахер Ф.Р.* Теория матриц. – М.: Наука, 1967.– 575 с. 4. *Глазман И.М., Любич Ю.И.* Конечномерный линейный анализ в задачах. – М.: Наука, 1969. – 476 с. 5. *Глухов В.С.* Порівняння поліноміального і нормального базисів представлення елементів полів Галуа // Вісн. Нац. ун-ту "Львівська політехніка". – 2007. – № 591. – С. 22–27. 6. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння: ДСТУ 4145: 2002. [чинний від 01.07.2003-07-01] – К.: Держ. комітет України з питань технічного регулювання та споживчої політики; 2003. – 38 с. – (Національний стандарт України). 7. *Курош А.Г.* Курс высшей алгебры. – М.: Наука, 1965. – 432 с. 8. *Мальцев А.И.* Основы линейной алгебры. – М.: Наука, 1970. – 423 с. 9. *Степанов С.А., Шпарлинский І.Е.* О построении примитивного нормального базиса конечного поля // Мат. сборник. – 1989. – Т. 180, № 8. – С.1067–1072. 10. *Фаддеев Д.К., Фаддеева В.Н.* Вычислительные методы линейной алгебры. – СПб.: Лань, 2002. – 733 с. 11. *Cohn H., Kleinberg R., Szegedy B., Umans C.* Group-theoretic Approach for Matrix Multiplication. http//arxiv.org. math/ 051F60v1 [math. GR] 18 Nov. 2005. 12. *Coppersmith D., Winograd S.* Matrix multiplication via arithmetic progressions // Symbolic Computation. – 1990. – № 9. – P. 251–280. 13. *Von Shur Gathen G., Giesbrecht M.* Constructing normal bases in finite fields // J. Symbolic Computation. – 1990. – № 10. – P. 547–570. 14. *Gao Sh.* Normal Bases over Finite Fields: Ph. thesis in Combinatorics and Optimization. – Waterloo, 1993. – 119 p. 15. *Stepanov S.A., Shparlinskiy I.E.* On construction of primitive elements and primitive normal bases in a finite field // Computational Number Theory / Ed. A. Peth, M.E., Pohst, H.C. Williams, H.G. Zimmer, 1991. (Proc. Colloq. Comp. Number Theory, Hungary, 1990). – P. 189–192.

Надійшла до редколегії 15.10.2010 р.

УДК 517.98

Г. Ющенко, асп.

ПРО СУМОВНІСТЬ ЗІ СТЕПЕНЕМ *P* РЕКУРЕНТНОЇ ПОСЛІДОВНОСТІ

Отримано критерій сумовності зі степенем p рекурентної послідовності.
We obtain a criterion for the recurrent sequence to be p-th power summable.

1. Формулювання основного результату

Нехай X – комплексний банахів простір з нормою $\|\cdot\|$, I, O – відповідно одиничний та нульовий оператори в X. Зафіксуємо $p \in [1;\infty)$ і покладемо

$$\ell_p(X) := \{x = \{x_n : n \ge 1\} \subset X \mid \|x\|_p := (\sum_{n=1}^{\infty} \|x_n\|^p)^{1/p} < \infty\}.$$

Відзначимо, що простір $\ell_p(X)$ з покоординатним додаванням і множенням на комплексний скаляр є комплексним банаховим простором.

Нехай A, B – лінійні обмежені оператори, які діють з X в X. Розглянемо послідовність, задану рекурентним співвідношенням

$$\begin{cases} x^{(0)} = \alpha \\ x^{(n)} = Ax^{(n-1)} + By^{(n)},\ n \ge 1, \end{cases} \tag{1}$$

де $\alpha \in X$ і $y = \{y^{(n)} : n \ge 1\} \in \ell_p(X)$.

Досліджується питання про умови на оператори A і B, за яких для кожної послідовності $\{y^{(n)} : n \ge 1\} \in \ell_p(X)$ і кожного $\alpha \in X$ послідовність $\{x^{(n)} : n \ge 1\}$, що визначається формулою (1), також належить простору $\ell_p(X)$.

Основний результат статті містить наступна теорема.

Теорема 1. Послідовність $\{x^{(n)} : n \geq 1\}$, задана співвідношенням (1), належить простору $\ell_p(X)$ для довільного $\{y^{(n)} : n \geq 1\} \in \ell_p(X)$ та $\alpha \in X$ тоді і тільки тоді, коли для спектрального радіуса $r(A)$ оператора виконується нерівність $r(A) < 1$.

Аналогічне питання щодо обмеженості такої послідовності при $B = I$ досліджувались в роботах [2, 3]. Слід зауважити, що в загальному випадку умови належності послідовності простору $\{y^{(n)} : n \geq 1\}$ відрізняються від умов, що забезпечують обмеженість цієї послідовності. Наприклад, послідовність (1) буде обмеженою, якщо $A = I,\ B = O$, хоча умова $r(A) < 1$ не виконується.

2. Доведення теореми 1

З формули (1) за допомогою методу математичної індукції отримуємо явний вираз для $x^{(n)}$:

$$x^{(n)} = A^n \alpha + A^{n-1} B y^{(1)} + \ldots + B y^{(n)},\ n \geq 1.$$

Розглянемо такі випадки.

1) $r(A) < 1$. Використовуючи теорему про спектральний радіус оператора дістанемо

$$\lim_{n\to\infty} (\| A^n \|)^{1/n} = r(A) < 1.$$

Тому існують такі $n_0 \in N$ і $q < 1$, що для кожного $n \geq n_0$ виконується нерівність $(\| A^n \|)^{1/n} < q < 1$. Звідси

$$\sum_{n=0}^{\infty} \| A^n \| \leq \sum_{n=0}^{k} \| A^n \| + \sum_{n=k}^{\infty} q^n < \infty. \qquad (2)$$

Нехай $\| B \| \neq 0$. Оцінимо норму $x^{(n)}$:

$$\| x^{(n)} \| \leq \| A^n \| \cdot \| \alpha \| + \| A^{n-1} \| \cdot \| B \| \cdot \| y^{(1)} \| + \ldots + \| B \| \cdot \| y^{(n)} \| = \| B \| \sum_{k=0}^{n} \| A^k \| \cdot \| y^{(n-k)} \|,\ n \geq 1,$$

де в останній рівності позначено $y^{(0)} := \alpha / \| B \|$. Перевіримо, що послідовність $\{x^{(n)} : n \geq 1\}$ справді належить $\ell_p(X)$. При $p \in (1, \infty)$ використовуючи властивості рядів, оцінку (2) та нерівність Гельдера дістанемо

$$\sum_{n=0}^{\infty} \| x^{(n)} \| \leq \| B \|^p \sum_{n=0}^{\infty} \Big(\sum_{k=0}^{n} \| A^k \| \cdot \| y^{(n-k)} \|\Big)^p \leq \| B^p \| \sum_{n=0}^{\infty} \Big(\sum_{k=0}^{n} \| A^k \| \cdot \| y^{(n-k)} \|^p\Big)^{1/p} \Big(\sum_{k=0}^{n} \| A^k \|\Big)^{1/q}\Big)^p =$$

$$= \| B^p \| \sum_{n=0}^{\infty} \Big(\sum_{k=0}^{n} \| A^k \| \cdot \| y^{(n-k)} \|^p \ \Big(\sum_{k=0}^{n} \| A^k \|\Big)^{p/q}\Big) \leq \| B^p \| \sum_{n=0}^{\infty} \Big(\sum_{k=0}^{\infty} \| A^k \| \cdot \| y^{(n-k)} \|^p \ \Big(\sum_{k=0}^{\infty} \| A^k \|\Big)^{p/q}\Big) \leq$$

$$\leq \| B^p \| \sum_{k=0}^{\infty} \| A^k \| \sum_{n=0}^{\infty} \| y^{(n)} \|^p \ \Big(\sum_{k=0}^{n} \| A^k \|\Big)^{p/q} < \infty$$

Тут q таке число, що $1/q + 1/p = 1$.

При $p = 1$

$$\sum_{n=0}^{\infty} \| x^{(n)} \| \ \leq \| B \| \sum_{n=0}^{\infty} \Big(\sum_{k=0}^{n} \| A^k \| \cdot \| y^{(n-k)} \|\Big) = \| B \| \sum_{k=0}^{\infty} \Big(\sum_{n=k}^{\infty} \| A^k \| \cdot \| y^{(n-k)} \|\Big) \leq \| B \| \sum_{k=0}^{\infty} \| A^k \| \sum_{n=0}^{\infty} \| y^{(n)} \| < \infty.$$

Якщо $B = O$, то відповідні оцінки тривіальні.

Отже, умова $r(A) < 1$ є достатньою для того, щоб для довільної послідовності $\{y^{(n)} : n \geq 1\} \in \ell_p(X)$ і довільного $\alpha \in X$ задана рівнянням (1) послідовність $\{x^{(n)} : n \geq 1\}$ належала простору $\ell_p(X)$.

2) $r(A) \geq 1$. Покажемо, що в цьому випадку можна вибрати такі $\alpha \in X$ і послідовність $\{y^{(n)} : n \geq 1\} \in \ell_p(X)$, що відповідна до них згідно з (1) послідовність $\{x^{(n)} : n \geq 1\}$ не належить $\ell_p(X)$.

Покладемо $D(C) = \{x \in X : (x, Ax, \ldots, A^k x, \ldots) \in \ell_p(X)\}$ і визначимо лінійний оператор $C : D(C) \to \ell_p(X)$ за правилом $Cx = (x, Ax, \ldots, A^k x, \ldots),\ \ x \in D(C)$. Доведемо, що $D(C) \neq X$ при $r(A) \geq 1$.

Якщо $r(A) = 1$, то внаслідок теореми про граничну точку спектра із [1, с.44-45] існують таке $\lambda \in \sigma(A), |\lambda| = 1$ і послідовність $\{x_n : n \geq 1\} \subset X$, що $\| x_n \| = 1,\ n \geq 1$ і $\| (A - \lambda I) x_n \| \to 0,\ n \to \infty$. Тому для кожного фіксованого $k \geq 1$ виконується $\| (A^k - \lambda^k I) x_n \| \leq \| A^{k-1} + \ldots + \lambda^{k-1} I \| \cdot \| (A - \lambda I) x_n \| \to 0,\ n \to \infty$, звідки

$$\big| \| A^k x_n \| - \| \lambda^k x_n \| \big| \leq \| (A^k - \lambda^k I) x_n \| \to 0,\ n \to \infty.$$

Оскільки $\| \lambda^k x_n \| = 1,\ k \geq 1,\ n \geq 1$, то $\| A^k x_n \| \to 1$ для кожного фіксованого $k \geq 1$ при $n \to \infty$. Тому для довільного $m \in N$ існує таке n, що $\| A^k x_n \|^p \geq 1/2$ для всіх $k = 1, \ldots 2m$, а отже $\| C x_n \|_p^p = \sum_{k=1}^{\infty} \| A^k x_n \|^p \geq m.$ Таким чином, оператор C – необмежений.

Якщо $r(A)>1,$ то з формули для спектрального радіусу дістанемо $\| A^n \| \to \infty,\ n\to\infty$. Звідси випливає необмеженість оператора C.

Покажемо, що C – замкнений оператор. Нехай $x_n \to x,\ n\to\infty$, де $\{x_n\}\subset D(C)$, і

$$\overline{f}_n = Cx_n = (x_n, Ax_n, ..., A^k x_n, ...) \to \overline{f} = (f^{(1)}, f^{(2)}, ..., f^{(k)}, ...) \in \ell_p(X),\ n\to\infty.$$

Тоді $A^k x_n \to f^{(k)},\ n\to\infty$ тобто $f^{(k)} = A^k x,\ k\ge 0.$ Отже, $\overline{x} = (x, Ax, ...A^k x, ...) \in D(C)$ і $\overline{f} = C\overline{x}$. З теореми про замкнений графік випливає, що оператор C не може бути визначений на всьому просторі. Отже існує таке $z\in X$, що $Cz = (z, Az, ..., A^k z, ...)$ не належить $\ell_p(X)$. Залишилось зауважити, що відповідна до $\alpha = z,\ y^{(k)} = 0,\ k\ge 1,$ послідовність $\{x^{(n)} : n\ge 1\}$ не належить $\ell_p(X)$. Теорему 1 доведено.

3. Висновки

Відомо, що при $B = I$ умова $r(A) < 1$ є необхідною і достатньою як для обмеженості послідовності (1) для кожного $\alpha\in X$ і кожної обмеженої послідовності $\{y^{(n)} : n\ge 1\}$, так і для її сумовності з p–им степенем для довільних $\alpha\in X$ і $\{y^{(n)} : n\ge 1\}\in \ell_p(X)$. У даній роботі встановлено, що результат щодо сумовності з p–им степенем послідовності (1) залишається правильним у випадку довільного лінійного обмеженого оператора B.

1. *Далецкий Ю.Л., Крейн М.Г.* Устойчивость решений дифференциальных уравнений в банаховом пространстве. – М.: Наука, 1970. 2. *Ким В.С.* Об условиях существования огранниченых решений разностного уравнения в банаховом пространстве // Дифференциальные уравнения. – 1967. – Т. 3, № 12. – С. 2151–2160. 3. *Томилов Ю.В.* Асимптотическое поведение одной рекурентной последовательности в банаховом пространстве // Асимптотичне інтегрування нелінійних рівнянь. – К., 1992. – С. 146–153.

Надійшла до редколегії 23.12.2010 р.

УДК 517.9 + 53(092)

М. Граб, асп.

ДІЯЛЬНІСТЬ КИЇВСЬКОГО УНІВЕРСИТЕТУ У РОКИ ДРУГОЇ СВІТОВОЇ ВІЙНИ

Проаналізовано архівні документи Київського національного університету імені Тараса Шевченка 1941–1943 років, розглянуто діяльність університету під час евакуації до м. Кзил-Орда Казахської РСР.

Archive data of Kyiv National Taras Shevchenko University for period 1941 – 1943 years are analyzed; activities of Kyiv University in evacuation to Kzyl-Orda of Kazakh Republic are considered.

1. Вступ

Найскладнішим періодом розвитку Київського університету, без сумніву, стали воєнні роки (1941–1943 рр.), протягом яких університет зазнав значних руйнувань, було знищено лабораторне обладнання, втрачено культурні цінності. Багато працівників університету поповнили лави Червоної Армії, дехто змушений був евакуюватися окремо від університету. Евакуація університету протягом 1941–1943 рр. сприяла швидкому відновленню університету в повоєнний час. Проте за роки війни було втрачено важливу облікову документацію, зокрема, яка стосується діяльності університету до 1939 року, також втрачено частину документів воєнного періоду, в яких йдеться про діяльність університету під час евакуації в 1943 році. Але з допомогою документів, які збереглися в архіві Київського національного університету імені Тараса Шевченка, зокрема, це деякі накази ректора за 1941–1942 роки, частково можливо висвітлити діяльність Київського університету під час евакуації у роки Другої світової війни. В документах за 1943 рік йдеться про відновлення діяльності університету після звільнення Києва від фашистських окупантів.

У даній статті проаналізовано архівні документи Київського національного університету імені Тараса Шевченка 1941–1943 років, а також висвітлено діяльність Київського університету напередодні та під час евакуації у роки Другої світової війни. Дана стаття доповнює попередні роботи автора [8, 9].

2. Київський університет і початок Великої Вітчизняної війни

У 1941 році Київський державний університет ім. Т. Г. Шевченка посідав третє місце за величиною серед університетів колишнього СРСР, поступаючись лише Московському та Ленінградському університетам. У Київському університеті функціонувало 9 факультетів: фізичний (декан – доцент М. Є. Гуртовий), механіко-математичний (в.о. декана – старший викладач І. Г. Ільїн), хімічний (декан – професор П. З. Фішер), геолого-географічний (декан – доцент І. Ф. Мукомель), біологічний (декан – доцент О. П. Корнеєв), історичний (декан – доцент П. А. Лавров), юридичний (декан – професор М. М. Гершонов), філологічний (декан – професор М. К. Грунський), факультет західних мов (декан – доцент С. Ю. Гальперн) [3, Л. 20–21]. До професорсько-викладацького складу належали 290 науково-педагогічних працівники, серед них: 9 академіків, 42 професори, 81 доцент, 32 старших викладачі, 71 викладач, 55 асистентів [4, Л. 32–40].

Проте Друга світова війна, що вирувала у Європі, вже наближалася до кордонів СРСР. Доказом того, що керівництвом держави було вжито різних заходів по підготовці до можливої майбутньої агресії з боку Німеччини, є наказ ректора Київського державного університету ім. Т.Г.Шевченка від 19 травня 1941 року, № 181, який було прийнято згідно з наказом Наркома Освіти УРСР С.В.Бухало від 15 травня 1941 року, № 1378. Відповідно до цього наказу з 5 по 27 червня 1941 року при Київському університеті повинні були відбутися навчальні збори військових керівників і викладачів військових дисциплін. Завідувач кафедри військової підготовки повинен був протягом трьох днів підготовити проект розташування слухачів зборів по аудиторіях, забезпечення їх зброєю, підручниками та наочним приладдям. Вказане забезпечення проводилося за рахунок фондів кафедр військової підготовки та фізичної підготовки [3, Л. 40].

З 23 червня 1941 року розпочалася мобілізація до лав Червоної Армії викладачів та студентів. Про це йдеться в наказах ректора Київського державного університету ім. Т. Г. Шевченка [4, Л. 71–94], [6, Л. 3–31].