УДК 512.642 + 512. 647 + 519.9

Р. Скуратовський, асп.

ПОБУДОВА НОРМАЛЬНОГО БАЗИСУ СКІНЧЕННОГО ПОЛЯ ЗА ДЕТЕРМІНОВАНИЙ ПОЛІНОМІАЛЬНИЙ ЧАС

Описано ефективний метод пошуку нормального базису в полі F_q над полем F_p. Складність методу оцінена зверху як $O(n^3)$, якщо елементарними операціями вважати арифметичні дії в полі F_q. Метод є детермінованим, тобто на відміну від багатьох відомих алгоритмів пошуку нормального базису він використовує не більше ніж $O(n^3)$ операцій у всіх випадках, а не в середньому.

Effective technique of finding normal basis in field F_q over field F_p is given. Complexity of the technique is about $O(n^3)$ if elementary operations are arithmetic operations in field F_q. The technique is determine that distinct it from many well known algorithms of finding the normal basis. The technique uses no more $O(n^3)$ operations in any case.

1. Вступ

Нормальний базис є зручним для обчислень, наприклад, для знаходження сліду елемента, розв'язання квадратних рівнянь над скінченним полем, тощо. Операція піднесення до квадрату у полі F_{2^n} є лише циклічним зсувом координат у нормальному базисі над F_2 [5]. На операції піднесення до квадрату базуються деякі обчислення в групі точок еліптичної кривої над скінченним полем, що може бути використано в алгоритмі цифрового підпису на еліптичній кривій над полем F_{2^n} [6].

У даний час однією з важливих задач криптоаналізу є розробка ефективних алгоритмів побудови нормального базису, яка проводиться за допомогою ймовірнісних і детермінованих методів. Найкращий з ймовірнісних методів [1] побудови нормального базису має складність $O\left(n^3+n^2 log^2 p\right)$. У [12] дано детермінований алгоритм, складність якого складає $O\left(n^4 \sqrt{p}\right)$. Серед детермінованих алгоритмів найкращими є алгоритми Льонстри і Лунберга [13], складність яких становить $O\left(n^4\log^2 p+n^2\log^3 p\right)$. Остання оцінка отримана за умови наявності незвідного полінома малої ваги над скінченним полем, наявність якого в таблиці незвідних поліномів не гарантована, а задача його знаходження є складною. У даній статті запропоновано новий метод побудови нормального базису в F_q, де $q=p^n$. Метод ґрунтується на теорії λ-матриць і нормальної форми Фробеніуса, його складність для довільного скінченного поля є $O\left(n^3 \log^2 q\right)$.

2. Означення і основні результати

Базис $\left(f_1, ..., f_n\right)$ називається нормальним, якщо $f_i = f_{i-1}^p$ для всіх $i = 2,...,n$. Оскільки елементи поля F_q подаються у вигляді векторів над F_p, то при побудові нормального базису спочатку будується оператор A піднесення до степеня в звичайному базисі, а потім знаходиться базис, в якому цей оператор є подібним до оператора B циклічного зсуву.

Відомо [1], що складність побудови поліноміального базису для F_q менша за n^3. Для побудови поліноміального базису треба знайти хоча б один корінь незвідного полінома і спряжені в F_q до нього корені. У випадку пошуку примітивного нормального базису треба аби $\overline{f_1}$ був примітивним елементом. Складність пошуку примітивного елемента в F_q, як встановив Ердеш [10], пов'язана з перебором $O\left(\sqrt{p}\ln^{17} p\right)$ елементів. Як зазначено у [10], згодом ця оцінка була покращена Ван Юанем до $O\left(p^{1/4+\varepsilon}\right)$ операцій. При переборі $n-\varphi\left(p^n-1\right)+1$, де $\varphi(m)$ –функція Ейлера [2], елементів з F_q серед них обов'язково можна знайти примітивний. Перевірка примітивності [14] довільного елемента $\theta\in F_q$ з використанням алгоритму факторизації може бути виконана за $O\left(p^{\varepsilon}\right), \varepsilon>0$, операцій, тому складність такої перевірки менша за $O\left(n^3\right)$. Мінімальний поліном $\mu(x)$ для елемента $\theta\in F_q$ згідно методу Берлікемпа-Месі [1] визначається за $O\left(n^2\right)M\left(log_2 p\right)$ операцій.

Складність [1, с. 170] алгоритму зведення за модулем незвідного полінома така ж, як і складність алгоритму множення цих поліномів, що за методом Карацуби становить $M(n)\le Cn^{\log 3}$, де C – деяка стала. Опишемо спочатку побудову оператора A піднесення до степеня в F_q. Нехай θ – знайдений вище примітивний елемент. Піднесемо елемент θ до степеня p, використовуючи бінарний алгоритм піднесення до степеня зі скануванням степеня зліва направо. На це йде, $\left[log_2 p\right]+\nu(p)$ множень, де $[x]$– ціла частина числа x, $\nu(p)$ – кількість одиниць у записі числа p. Таким чином маємо оцінку $O\left(n^2\right)+\left[log_2 p\right]+\nu(p)$ для обчислення елемента θ^p.

Для перевірки примітивності довільного елемента θ з поля F_q достатньо перевірити чи не є його порядок одним з порядків підгруп мультиплікативної групи поля F_q. Позначимо мінімальний з таких порядків m_0, а $y = \left(p^n - 1\right)/m_0$. Тому складність пошуку примітивного елемента θ можна оцінити як

$$\left(n - \varphi\left(p^n - 1\right) + 1\right)\left(\left([log_2 y] + \nu(y)\right)\log_2\left(p^n - 1\right)\log_2 m_0\right).$$

Далі знаходимо $\theta^{2p} = \theta^p\theta^p, \ldots, \theta^{(n-1)p}$. При цьому при $kp < n$ на $(kp+1)$-ому місці в векторному записі елемента $\theta^{kp} \in F_q$ поля F_q буде стояти 1, а на інших місцях – нуль.

У випадку $kq \ge n$ при обчисленні елемента θ^{kp}, $k < n$, виконуємо їх зведення за модулем незвідного полінома $\mu(x)$ над полем F_p, а потім знаходимо зображення цих елементів у вигляді векторів над F_p. Кількість стовпців отриманих елементів дорівнює n і співпадає з кількістю елементів нормального базису. Таким чином отримані вектори визначають деяку матрицю $M \in GL[n]$, яка задає оператор A. Отже, загальний час знаходження оператора A піднесення до степеня у довільному базисі становить

$$T = O\left(\sqrt{p}\ln^{17} p\right) + O\left(p^{\varepsilon}\right) + [log_2 p] + \nu(p) + (np - n + 1)M(n), \text{ де } q = p^n.$$

Покажемо, що многочлен $x^n - 1$ є мінімальним многочленом для оператора A. Оскільки, для кожного $f \in F_q$ маємо $A^n f = f^{q^n} = f$, то A^n є тотожним оператором, тобто $A^n = I$. Добре відомо [8], що оператор $\mathrm{A}f = f^p$, де $f \in F_q$, є лінійним над полем F_q. Доведемо, що n – мінімальна степінь. Для довільного многочлена $P(x) = a_m x^m + \ldots + a_1 x + a_0$, де $m < n$, справедливе відношення $P(\mathrm{A})f = Q(f)$, де $Q(f) = a_m f^{p^m} + \ldots + a_1 f^p + a_0 f$ – елемент поля F_q, $deg\, P(f)$ не вище, ніж q^{n-1}. Тому поліном $P(x)$ має не більше, ніж p^{n-1} коренів. Це означає, що існує такий елемент $f \in V\left(F_q\right)$, де $dim V = n$, що $P(A)f = Q(f) \ne 0$, звідки $P(A) \ne 0$, що суперечить означенню мінімального полінома [8], тобто $P(x)$ не мінімальний. Тому $x^n - 1$ є мінімальним поліномом оператора A над полем F_q. Оператор A побудовано за матрицею M, яка є простою [4], бо її мінімальний поліном співпадає з характеристичним.

Означення. Циклічним вектором називається такий вектор $\vec{c}$, що вектори $\vec{c}$, $A\vec{c}, \ldots, A^{n-1}\vec{c}$ є лінійно незалежними, тобто утворюють базис простору V. Очевидно, що такий вектор існує тоді й тільки тоді, коли оператор A є простим [4].

Для кожного вектора $\vec{c}$ лінійна оболонка *L* системи векторів $\vec{c}$, $A\vec{c}, \ldots, A^{n-1}\vec{c}$ є інваріантним підпростором, який називається циклічним підпростором, що породжений вектором $\vec{c}$. Очевидно, що циклічний вектор у випадку простого оператора існує, бо з критерію цикличності простору слідує, що такий вектор існує тоді й тільки тоді, коли оператор A простий. Цим доцільно скористатися при побудові нормального базису поля. Ступінчастою матрицею називається квадратна матриця N, на діагоналі якої містяться квадратні блоки D_{ii} (у даному випадку D_{ii} є клітинами Фробеніуса), а D_{ij} при $i > j$ є нульовими, тобто $N = \begin{pmatrix} D_{11} & B_{12} & B_{13} \\ 0 & D_{22} & B_{23} \\ 0 & 0 & D_{33} \end{pmatrix}$.

Анулятором вектора $\vec{u}$ називається анулюючий його матричний поліном мінімальної степені. Він позначається $Ann_M(\vec{u})$. Анулятором простору U називається анулюючий його матричний поліном мінімальної степені. Він позначається $Ann_M(U)$.

Знайдемо циклічний вектор у полі F_q. Нехай методом Данілєвського [9] знайдено матрицю *M,* яка у загальному випадну вона є багатоступінчатою. Двоступінчатій матриці M відповідає оператор, який є напівпрямою сумою операторів, що визначаються матрицями C_1, C_2, тобто матриці M задає оператор A, який є розширенням оператора, що визначається матрицею C_1, за допомогою оператора, що визначається матрицею C_2, тобто

$$M\vec{u}_1 = \begin{pmatrix} C_1 & B \\ 0 & C_2 \end{pmatrix}\vec{u}_1 = \left(g_1, g_2, \ldots, g_k, 0, \ldots, 0\right)^T,$$

де C_1, C_2 – клітини Фробеніуса розмірів $k \times k$ і $l \times l$ відповідно, $\vec{u}_1 = (1, \ldots, 0, \ldots, 0)^T = \vec{e}_1^{\,T}$.

Вектор $\vec{u}_1$ є циклічним для інваріантного підпростору $U_1 = \left\langle e_1, Me_1, \ldots, M^k e_1\right\rangle = \left\langle e_1, e_2, \ldots, e_k\right\rangle$. Позначимо $\vec{u}_2 = \left(\underbrace{0, \ldots, 0}_{k}, \underbrace{1, \ldots, 0}_{l}\right)^T = \vec{e}_{k+1}^{\,T}$.

Нехай $\vec{v}_2$ – вектор з останніх $n-k$ координат вектора $\vec{u}_2$. Тоді $M\vec{u}_2 = (*,...,*,0,1,0,...,0)$, $M^2\vec{u}_2 = (*,...,*,0,0,1,0,...,0)$, …, $M^l\vec{u}_2 = (*,...,*,0,0,...,0,1)$, …, $M^n\vec{u}_2 = (*,...,*,C^n\vec{v}_2)$. Лінійна оболонка цієї системи векторів є інваріантним підпростором, який позначимо U_2, де $l \le dimU_2 \le n$. Позначимо $P(x) = Ann_M(U_1)$, $Q(x) = Ann_M(U_2)$. Зауважимо, що $P(x) = \det(A - Ex)$, де E – одинична матриця, а $P(x)$ – анулятор інваріантного підпростору U_1 і породжучого його вектора $\vec{u}_1$. У випадку, коли найбільший спільний дільник $P(x),\ Q(x)$ не рівний 1, тобто $(P(x), Q(x)) \ne 1$, знайдемо анулятор для вектора $\vec{u}_2 = \vec{e}_{k+1}$ розмірності $n = k + l$.

Лема 1. Для простої матриці M, яка перетворена методом Данілєвського до двоступінчатого вигляду, можна знайти анулятор вектора $\vec{u}_2 = \vec{e}_{k+1}$ для клітини C_2 за $O(n^3)$ операцій.

Доведення. Позначимо через $\vec{g}_i$ зведені вектори, що отримані під дією M. У загальному випадку $\vec{g}_1 = \vec{e}_{k+1} = (0,...,0,1,0,...,0)$, $\vec{g}_2 = M\vec{e}_{k+1} - c_1\vec{g}_1$, бо щонайбільше одну з координат вектора $M\vec{e}_{k+1}$ можна занулити відніманням $\vec{g}_1$. Занулимо за допомогою отриманих $\vec{g}_1$ і $\vec{g}_2$ вже дві координати вектора $M^2\vec{e}_{k+1}$. Маємо $M^2\vec{e}_{k+1} - c_1\vec{g}_1 - c_2\vec{g}_2 = (v_1,...,v_{k-1},0,v_{k+1},..,0,.,v_m)$, $M^3\vec{e}_{k+1} - c_1\vec{g}_1 - c_2\vec{g}_2 - c_3\vec{g}_3 = (v_1,.,0,..,v_{k-1},0,v_{k+1},..,0,.,v_m)$. Цей процес можна продовжити до *m*-го кроку і отримати $\vec{g}_{m+1} = M^m\vec{e}_{k+1} - c_1\vec{g}_1 - c_2\vec{g}_2 - c_3\vec{g}_3 - ... - c_m\vec{g}_m = (0,...,0,..,0)$. Тепер виразимо $\vec{g}_i$ через $M^{i-1}\vec{e}_{k+1}$. Це дає аннулятор $Q(x)$. При цьому, для обчислення значення $M^i\vec{e}_{k+1}$, де $i = \overline{2,m}$, $l \le m \le n$, використовується операція множення матриці на вектор, а не піднесення матриці до степеня, бо такий спосіб обчислень дозволяє зменшити кількість арифметичних операцій. Виразивши $\vec{g}_{m+1}$ через $M^{i-1}\vec{e}_{k+1}$, де $i = \overline{2,m}$, отримаємо $Q(x)$. Врахуємо те, що складність множення матриць, згідно алгоритму Кохна [10] є $O(n^{2,41})$, за методом Виноград- Коперстміта [11] – $O(n^{2,376})$, що при кратному піднесені до степеня дасть більше ніж $O(n^3)$, а складність множення матриці на вектор – $O(n^2)$. Оскільки $M \in GL[n]$, то описане вище занулення завжди можливе. Лему1 доведено.

Приклад. Розглянемо матрицю $M = \begin{pmatrix} C_1 & B \\ 0 & C_2 \end{pmatrix}$, де $C_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, $C_2 = \begin{pmatrix} 0 & 5 \\ 1 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 3 \\ 0 & 2 \end{pmatrix}$. Через $\vec{g}_i$ позначимо перетворені вектори, що отримані під дією M, після застосування методу зведення Гаусса. Отже $\vec{g}_1 = \vec{e}_{k+1} = (0,0,1,0,0)$, $\vec{g}_2 = M\vec{e}_{k+1} = (2,0,0,1)$, $M^2\vec{e}_{k+1} = (3,4,5,3)$. Далі занулюємо вже дві координати $\vec{g}_3 = M^2\vec{e}_{k+1} - 5\vec{g}_1 - 3\vec{g}_2 = (-3,4,0,0)$, $\vec{g}_4 = M^3\vec{e}_{k+1} - 5\vec{g}_1 - 14\vec{g}_2 - 5/3\vec{g}_3 = (0,\ 19/13,\ 0,\ 0)$. Звідси знаходимо $Q(x) = M^4\vec{e}_{k+1} - d\vec{g}_4 - c\vec{g}_3 - b\vec{g}_2 - a\vec{g}_1$.

Зауваження 1. $Q(x)$ можна знайти швидше. Для цього спочатку потрібно обчислити вектор $\vec{w} = \chi_C(M)\vec{u}_2$. У вектора $\vec{w}$ останні l координат рівні 0, бо на них діє лише блок C_2, для якого $\det(C_2 - Ex)$ є дільником $Q(x)$ [7]. З перших k координат вектора $\vec{w}$ побудуємо вектор $\vec{w}_1$ і застосовуємо метод занулення вектора, що описаний вище. Отримаємо $Pol_A(A)\vec{w}_1 = Pol_A(M)\vec{w}_1$, але у $\vec{w}$ занулені останні l координат. Це матричний поліном меншої степені ніж у $Q(x)$ і він занулює вектор меншої розмірності, тому маємо суттєве прискорення. Отже $Q = Pol_A(M)\chi_C(M)\vec{u}_2$.

Далі знайдемо такі взаємно прості над полем F_q поліноми $P_0(x), Q_0(x)$, що $Q(x) = Q_1(x)Q_0(x)$, $P(x) = P_1(x)P_0(x)$, найменше спільне кратне яких співпадає з анулятором простору V, тобто $\text{НСК}(P_0(x), Q_0(x)) = Ann_M V$.

Опишемо метод побудови поліномів $P_0(x), Q_0(x)$ за $P(x), Q(x)$. На першому кроці знаходимо $(P(x), Q(x)) = R(x)$ і визначаємо домінантну частину незвідних поліномів в $P(x)$ відносно $Q(x)$ – поліном $p_1(x) = P(x)/R(x)$. Якщо $p_1(x)$ є сталою, то $P_0(x) = p_1(x)$. Якщо це не так, то знаходимо $p_2(x) = (p_1(x), R(x))$. Якщо $p_2(x)$ є сталою, то $P_0(x) = p_1(x)p_2(x)$. Якщо це не так, то далі ітеруємо за формулою $p_k(x) = (p_{k-1}(x), R(x)/(p_2(x)...p_{k-1}(x)))$, де $k = 2,...$. Зрозуміло, що цей процес скінчений і при деякому $d \in \mathbb{N}$ отримаємо $p_d(x)$ – стала. Нехай d – найменше таке число. Тоді шуканий поліном $P_0(x)$ має вигляд

$P_0(x)=p_1(x)p_2(x)\,...\,p_d(x)$. Зрозуміло, що $P_0(x)$ є дільником $P(x)$, а отже існує поліном $P_1(x)$ для якого маємо $P(x)=P_0(x)P_1(x)$. Поліном $Q_0(x)$ знаходимо аналогічно.

Обгрунтуємо побудову $P_0(x),\,Q_0(x)$. Нехай $P(x)=r_1^{i_1}(x)\,...\,r_s^{i_s}(x),\quad Q(x)=t_1^{j_1}(x)\,...\,t_m^{j_m}(x)$ – розклади на незвідні многочлени. Позначимо $K=\max\{s,\,m\}$. Доведемо, що степінь кожного незвідного полінома в розкладі $P(x)$ є однаковим для $\text{НСК}(P_0(x),\,Q_0(x))$ і $\text{НСК}(P(x),\,Q(x))$. Не втрачаючи загальності розглянемо поліном $P(x)$ і степінь незвідного полінома $r_1^{i_1}(x)$ в розкладі $P(x)$. Позначимо $\deg_1 P(x):=\deg r_1^{i_1}(x)=i_1$. Можна вважати, що $\deg_1 P(x)>\deg_1 Q(x)$.

Випадок 1. $\deg_1 p_1(x)>\deg_1 R(x)$. Тоді $p_2(x)=(p_1(x),R(x))$ і $\deg_1 p_2(x)=\deg_1 R(x)$. Звідси $\deg_1 p_1(x)p_2(x)=$ $=\deg_1 p_1(x)+\deg_1 R(x)$. Оскільки $p_1(x)=P(x)/R(x)$, то $\deg_1 p_1(x)p_2(x)=\deg_1 p_1(x)+\deg_1 R(x)=\deg_1 P(x)$, що і треба було довести. Зрозуміло, що у цьому випадку $\deg_1 q_1(x)=\deg_1(Q(x)/R(x))=0$.

Випадок 2. $\deg_1 p_1(x)\le\deg_1 R(x)$. Позначимо $[\deg_1 R(x)/\deg_1 p_1(x)]=d$. Зрозуміло, що $\deg_1 R(x)=j_1$. Тоді з рівності $p_2(x)=(p_1(x),R(x))$ слідує $\deg_1 p_2(x)=\deg_1 p_1(x)$, бо $\deg_1 p_2(x)=\min\{\deg_1 p_1(x),\deg_1 R(x)\}$. Тому степінь $r_1(x)$ однаковий в розкладі поліномів $p_2(x)$, $p_1(x)$ на незвідні многочлени. Тоді $\deg_1 p_3(x)=\min\{\deg_1 p_1(x),\deg_1(R(x)/p_2(x))\}=\;=\min\{\deg_1 p_1(x),\deg_1(R(x)/p_1(x))\}=\deg_1 p_1(x)$. При цьому $\deg_1(R(x)/p_1(x))=d-1$, бо відбулося одне ділення на $p_1(x)$, який містить $r_1^{i_1}(x)$. Тоді $\deg_1 p_4(x)=\min\{\deg_1 p_1(x),\deg_1(R(x)/p_1^2(x))\}=\deg_1 p_1(x)$, отже $\deg_1(R(x)/p_1^2(x))=d-2$. Цей процес продовжуємо далі. На (d+2)-ому кроці отримаємо

$$\deg_1 p_{d+2}(x)=\min\{\deg_1 p_1(x),\deg_1(R(x)/p_1^d(x))\}=\deg_1(R(x)/p_1^d(x))=\deg_1 R(x)-\deg_1(p_1^d(x)),$$

$$\deg_1 P_0(x)=\deg_1 p_1(x)p_2(x)...p_k(x)=\deg_1\left(p_1(x)p_2(x)...p_{d+1}(x)\left(R(x)/\left(p_1^d(x)\right)\right)\right)=$$

$$=\deg_1\left(p_1^{d+1}(x)\cdot\left(R(x)/\left(p_1^d(x)\right)\right)\right)=\deg_1(p_1(x)\cdot R(x))=\deg_1 P(x).$$

Тому в розкладі НСК$(P(x),Q(x))$ на незвідні поліноми степінь незвідного многочлена $r_1(x)$ буде таким, як і в НСК$(P_0(x),Q_0(x))$. Що і потрібно було довести. Аналогічно розглядаються випадки інших незвідних поліномів $r_i(x)$.

Якщо степінь незвідного полінома є більшим у $P(x)$, то він буде присутній у розкладі $P_0(x)$ з тим самим степенем. Зрозуміло, що у цьому випадку $\deg_1(q_1(x))=\deg_1 Q(x)/R(x)=0$. Тому $(P_0(x),Q_0(x))=1$. Процес ділення на цьому не завершується на $(d+2)$-ому кроці. Він триватиме $\tilde{k}=\max\limits_z\{|\deg_z R(x):\deg_z p_z(x)|\}$, де $\deg_z R(x)\ge\deg_z p_z(x)\ne 0,\ z\le s,\ z\in\mathbb{N}$ разів до виділення останнього незвідного многочлена $r_z^{i_z}(x)$, степінь якого в розкладі $P(x)$ є більшою, ніж $\deg_z R(x):=\deg r_z^{i_z}(x)=i_z$ – степінь $r_z(x)$ в розкладі $R(x)$ на незвідні многочлени.

Складність обчислення найбільшого спільного дільника для поліномів з степенями $\deg p(x)=d_1,\ \deg R(x)=d_2$ становить $O(d_1 d_2)$. Тому для матриці M таке обчислення складе не більше $O(n^2)$ кроків. Зауважимо, що $\tilde{k}\le n$ – це слідує з кількості кроків алгоритму. Для випадку $\deg_z p_1(x)\ge\deg_z R(x)\ne 0$ аналогічно показується, що $\tilde{k}\le n$. Отже маємо оцінку складності $O(n^3)$, де n – розмір двоступінчатої квадратної матриці M, з яких складається нормальна форма Фробеніуса N. Циклічним вектором відносно M є вектор $\overline{c}=Q_1(M)\overline{u_1}+P_1(M)\overline{u_2}$.

Лема 2. Для довільного інваріантного простору $H=\langle e_1, Me_1, M^2e_1,...,M^{k-1}e_1\rangle$ і простої матриці M виконується рівність $\deg(Ann_M H)=\dim H=k$.

Доведення. Позначимо $P(x)=Ann_M H$. Оскільки H – інваріантний підпростір, то розглянемо факторпростір $V/H=W$. Враховуючи $\dim H=k$, маємо $\dim W=n-k$. Скористаємося методом доведення від супротивного. Нехай $\deg(Ann_M H)<k$. Тоді, якщо виконується умова $\deg(Ann_M W)=n-k,$ то $\deg(P(x)\cdot Ann_M W)<n$. Але

$Ann_M V$ ділить $P(x) Ann_M W$, тому маємо протиріччя, бо для простої матриці згідно відомої теореми [4, с. 107] $\deg(Ann_M V) = n$.

Зауваження 2. Для простої матриці M виконується умова $P(x) \neq Q(x)$.

Доведення. Скористаємося методом доведення від супротивного. Якщо $P(x) = Q(x)$, то $P(x)$ є анулятором підпросторів U_1 і U_2, тому він зануляє весь простір V. За згаданою вище теоремою $\deg(Ann_M V) = n$. Тому $\deg(P(x)) \geq n$. Оскільки U_1 – інваріантний власний підпростір, то за лемою 2 $\deg P(x) = \deg(Ann_M U_1) = \dim U_1 = k < n$. Отже маємо протиріччя.

Зауваження 3. Якщо $Ann_M V = h^r(x)$, де $h(x)$ – незвідний поліном, то $Ann_M V = Q(x)$.

Доведення. Дійсно, з умов $\text{НСК}(P(x), Q(x)) = Ann_M V$ і $\deg P(x) = k$ слідує, що $\deg Q(x) = n$ і $\vec{e}_2$ – циклічний вектор у V. Випадок $Ann_M V = h^r(x)$ можливий лише за умови $n = lp,\ p = char(P)$.

Многочленам $P_0(x), Q_0(x)$ відповідають інваріантні підпростори $X = \left\{\vec{x} \middle| P_0(M)\vec{x} = \vec{0}\right\}$, $Y = \left\{\vec{y} \middle| Q_0(M)\vec{y} = \vec{0}\right\}$, $X, Y : X \cap Y = 0$, $X \oplus Y = V$. Оскільки $HCK(Ann_M X, Ann_M Y) = Ann_M V,\ (Ann_M X, Ann_M Y) = 1$, то $X \oplus Y = V$.

Циклічним вектором для підпростору X, очевидно, є вектор $\vec{v}_1$, бо $\vec{v}_1 = P_1(x)\vec{e}_1$. Порядок його анулятора збігається з розмірністю підпростора X. Крім того, $P_1(x)$ ділить $P(x)$, для підпростору Y вектор $\vec{v}_2 = Q_1(M)\vec{u}_2$ є циклічним. Циклічним вектором для підпростору U_1 є $\vec{e}_1$. Доведемо, що $\vec{c} = \vec{x} + \vec{y}$ циклічний у просторі V. Це слідує з наступної леми, що доведена в [3].

Лема 3. Якщо мінімальні поліноми $\mu_1(x), \mu_2(x)$ векторів $\vec{x}, \vec{y}$ взаємно прості, то мінімальним поліномом вектора $\vec{c} = \vec{x} + \vec{y}$ є $\mu_1(x)\mu_2(x)$.

Таким чином, $deg(Ann_M \vec{c}) = n$. Звідси легко отримується базис n-вимірного циклічного простору, що породжений вектором $\vec{c}$ під дією оператора *A*. Тому $\vec{c}$ – циклічний у просторі V. Розмірність циклічного простору рівна порядку циклічного вектора $\vec{c}$ відносно оператора A.

Лема 4. Об'єднати всі підпростори, яким відповідають клітини Фробеніуса, можна не більше ніж за $O(n^3)$ дій.

Доведення. Позначимо розміри сусідніх клітин Фробеніуса a і b. Тоді кількість операцій на отримання клітин a і b становить: $t(a) \leq 3a^3$, $t(b) \leq 3b^3$ і $3a^3 + 3b^3 + n^3 \leq 3n^3$, де n – розмір матриці N. Доведемо ці оцінки за індукцією по розмірності підпросторів, що утворилися після об'єднання. Випадок $\dim A = 1,\ \dim B = 1$ очевидний. Об'єднання клітин розміру більше ніж 1 на 1 робиться за кількість операцій, що пропорційна кубу суми розмірностей. Справді, для матриці M, що описана в Лемі 1, для отримання циклічного вектора $\vec{u}_1$ потрібно $O(n^3)$ елементарних операцій у полі F_q (див. Лему 1). Складність об'єднання двох клітин оцінено вище при обгрунтуванні алгоритму знаходження $P_0(x), Q_0(x)$.

Розглянемо випадок $a \leq 3n/4,\ b \geq n/4$. Позначимо $V(x)$ – підпростір розмірності x. Здійснимо перехід індукції для граничного випадку $a = n/4,\ b = 3n/4$. Маємо $\left(3\left(1/4\right)^3 + 3\left(3/4\right)^3 + 1\right)n^3 < 3n^3$.

Розглянемо тепер випадок $a > 3n/4,\ b < n/4$. Можливо два випадки: підпростір $V(a)$ є іманентним для отриманої нормальної форми Фробеніуса, або його отримано об'єднанням сусідніх клітин. Якщо $V(a)$ – іманентний, то на останньому кроці об'єднуються підпростори $V(a)$, $V(b)$, де $a > 3n/4$, $b < n/4$. Тут $V(b)$ отримано об'єднанням підпросторів, на що витрачено не більше ніж $3b^3$ операцій. Отже справджується оцінка $(a+b)^3 + 3b^3 = n^3 + 3b^3 < n^3 + 3\frac{n^3}{64} < 3n^3$.

Якщо підпростір $V(a)$, $a > 3n/4$, утворено в процесі об'єднання сусідніх клітин, починаючи з клітин меншої розмірності, то $V(a)$ отримано на передостанньому кроці. При цьому посередині був найбільший підпростір $V(d)$, а по краям – $V(c)$, $V(b)$, де $c < b$, $n/4 > c,\ n/2 > b > n/4$. Тому об'єднуються $V(c)$, $V(d)$ і маємо $(c+d)^3 + 3c^3 + 3b^3 + n^3 < 3n^3$, де $d > n/2$. При цьому підпростір $V(d)$ є іманентним, тому доданку $3d^3$ в останній 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.