УДК 519.176,519.157.2

В. А. Устименко

О K-теории динамических систем, соответствующих графам, и ее применении

(Представлено членом-корреспондентом НАН Украины А. Н. Трофимчуком)

Определяются некоторые классы зависимых от времени дискретных динамических систем. Определение мотивировано проблемами криптографии, основанной на полиномиальных преобразованиях от многих переменных, в частности, поиском циклических групп полиномиальных преобразований неограниченного порядка, образованных преобразованиями степени, не более 3. Существование определенных аксиомами дискретных динамических систем доказывается методами конструктивной экстремальной теории графов. Некоторые динамические системы определяются по построению новых примеров семейств графов большого обхвата суперлинейного размера. В частности, приводится конструкция такого семейства графов без реберно транзитивной группы автоморфизмов. Построены также новые примеры семейств графов с большим цикловым показателем.

О полиномиальной криптографии от многих переменных и стабильных группах преобразований. Поиск специальных дискретных динамических систем, зависящих от времени, мотивирован, в частности, задачами полиномиальной криптографии от многих переменных, в том числе проблемой нахождения последовательностей циклических групп полиномиальных преобразований неограниченного порядка от возрастающего колличества переменных, образованных преобразованиями степени меньше 4. Семейства образующих таких последовательностей циклических групп будем называть стабильными. Существование заданных аксиомами динамических систем доказывается методами экстремальной теории графов. В частности, используются новые конструкции простых и ориентированных графов большого обхвата и графов с большим цикленным показателем. Известно, что в случае $K = Fq$ наилучший алгоритм отыскания решения системы полиномиальных уравнений $f_i(x_1, x_2, \dots, x_n) = bi$, $i = 1, 2, \dots, n$, находящейся в "общем положении", имеет оценку сложности $d^{O(n)}$, где d — максимальная степень полиномов. Алгебраическая задача обращения полиномиального отображения $(x_1, x_2, \dots, x_n) \to$ $\to (f_1(x_1, x_2, \dots, x_n), f_2(x_1, x_2, \dots, x_n), \dots, f_n(x_1, x_2, \dots, x_n))$ является еще более сложной. Полиномиальная криптография от многих переменных изучает криптосистемы, безопасность которых основывается на сложности приведенных выше задач. Зачастую используется следующая общая схема алгоритма с публичным ключом.

Алиса (собственник ключа) использует набор нелинейных многочленов $G_1, G_2, \dots, G_s$ группы Кремоны $C(K^n)$, для которых вычислены обратные к ним полиномиальные отображения $G'_1, G'_2, \dots, G'_s$. Она вычисляет $F = T_1 G_1 G_2 \dots G_s T_2$, где T_1 и T_2 — биективные афинные преобразования свободного модуля K^n. Публичное правило $x_1 \Rightarrow f_1(x_1, x_2, \dots, x_n)$, $x_2 \Rightarrow f_2(x_1, x_2, \dots, x_n)$, $\dots$, $x_n \Rightarrow f_n(x_1, x_2, \dots, x_n)$, соответствующее отображению F, предоставляется пользователям. Если степень нелинейного преобразования ограничена константой, а параметр n принят за переменную, то пользователь (Боб) может кодировать за полиномиальное от n время.

Алиса хранит в безопасности отображения G_1, G_2, …, G_s и декодирует полученные шифрограммы при помощи $T_2'G_s'$, G_{s-1}', …, $G_1'T_1'$. Исторический обзор исследований, начиная от криптосистемы Имаи Мацумото и ее криптоанализа, найденного Я. Патариным, можно найти в [1]. Примеры использования последовательностей стабильных полиномов вместе с небольшим числом быстро вычислимых многочленов высокой степени, образующих символический ключ, приводится в [2, 3]. Семейство G_n стабильных кубических элементов большого порядка может использоваться для протокола обмена ключами по схеме Диффи–Хеллмана в случае циклической группы $\langle G_n\rangle$ преобразований модуля K^n.

Пользователи (Алиса и Боб) используют посланное по открытому каналу отображение G_n. Они выбирают их персональные ключи K_A (Алиса) и K_B (Боб), являющиеся достаточно большими натуральными числами. После этого пользователи обмениваются кубическими преобразованиями $G_n^{k_a}$ и $G_n^{k_b}$ соответственно. По завершению протокола Алиса и Боб могут использовать общее "публичное правило" $x_1 \Rightarrow g_1(x_1, x_2, \ldots, x_n)$, $x_2 \Rightarrow g_2(x_1, x_2, \ldots, x_n)$, …, $x_n \Rightarrow g_n(x_1, x_2, \ldots, x_n)$, соответствующее отображению $G_n^{k_ak_b}$, в виде списка коэффициентов у стандартном порядке или какой-либо быстровычислимой хаш-функции от полученного вектора.

Безопасность протокола основывается на трудности проблемы дискретного логарифма для циклической группы с образующей G_n. При определенных условиях возникает задача "скрытого дискретного логарифма" — для вычисления порядка циклической группы не хватает вычислительных ресурсов ([4] и дальнейшие ссылки).

О некоторых классах динамических систем. Пусть K — произвольное коммутативное кольцо. Последовательность элементов кольца $t_1, t_2, \ldots, t_s$ называется аддитивно устойчивой, если произведение d элементов $(t_i + t_{i+1})$, не равно нулю. Последовательность элементов кольца $t_1, t_2, \ldots, t_s$ назовем циклически антинильпотентной, если элемент $d(t_1 + t_s)$ является антинильпотентным, т. е. для любого натурального x элемент d^x отличен от нуля.

Пусть M — мультипликативное подмножество в K, т. е. замкнутое относительно умножения и не содержащее нуля. Тогда последовательность элементов $t_1 = t$, $t_2 = -t + m_1$, $t_3 = t - m_1 + m_2$, $t_4 = -t + m_1 - m_2 + m_3$, …, $t_s = -t_{s-1} + m_{s-1}$, где m_1, m_2, …, m_{s-1} — элементы из M, является аддитивно устойчивой при четном числе элементов. Для циклической нильпотентности достаточно добавить условие принадлежности $t + t_s$ множеству M.

Пусть P_n и L_n — две копии свободного модуля K^n. Семейства обратимых регулярных отображений D^nt, где t принадлежит K, алгебраического многообразия P_nUL_n назовем двудольной динамической системой большого обхвата, если

1) $x \in P_n \Rightarrow D^nt(x) \in Ln$, $x \in Ln \Rightarrow D^nt(x) \in Pn$;

2) $(D^nt)^{-1} = D^nt'$ для некоторого t' из K, отличного от нуля;

3) существует константа c, $c > 0$, такая, что для некоторой линейной функции $a(n) = cn + d$ композиция $D^nt_1t_2\cdots t_s$ преобразований D^nt_1, D^nt_2, …, D^nt_s, где $0 < s < a(n)$ и $t_1, t_2, \ldots, t_s$ — аддитивно устойчивая последовательность, выполняется условие отличия $D^nt_1t_2\cdots t_s(x)$ от $D^nr_1r_2\cdots r_j(x)$, для всех x из K и всех отличных от последовательностей $r_1, r_2, \ldots, r_j \in K^j$, $j < s + 1$;

4) пусть $t_1, t_2, \ldots, t_s$ — циклически антинильпотентная последовательность, тогда порядок элемента $D^nt_1t_2\cdots t_s$ стремится к бесконечности с ростом параметра n.

Заметим, что неравенство из условия *3* можно переписать в виде $D^nt_1t_2\cdots t_sr_j'r_{j-1}'\cdots$ $\cdots r_1'(x)$ отлично от x. Это означает, что отображения вида $D^nt_1t_2\cdots t_sr_1r_2\cdots r_j$, где t_1, t_2, …, t_s — аддитивно устойчивая последовательность и $r_1, r_2, \ldots, r_j$ не совпадает с t_s', $t_{s-1}', \ldots, t_1'$, не имеют неподвижных точек на P_nUL_n.

Заменив в условии *3* определения двудольной динамической системы большого обхвата квантор "для всех" x, $x \in P_nUL_n$ на условие существования x, $x \in P_nUL_n$, получим определение двудольной симметрической динамической системы большого цикленного показателя.

Если D_t такая система, то отображения $D^n t_1 t_2 \cdots t_s$ и $D^n r_1 r_2 \cdots r_j$, где t_1, t_2, ..., t_s — аддитивно устойчивая последовательность, а $j < s+1$ совпадают только при равенстве последовательностей t_1, t_2, ..., t_s и r_1, r_2, ..., r_j. Заменив в приведенных выше определениях алгебраические многообразия P_nUL_n (объединение двух копий свободного модуля K^n) на многообразие K^n, получим определения симметрической динамической системы большого обхвата и симметрической динамической системы с большим цикленным показателем.

Будем говорить, что введенные выше динамические системы являются кубическими, если все нетождественные преобразования вида $D^n t_1 t_2 \dots t_s$ являются полиномиальными отображениями третьей степени. Отметим, что обратные для $D^n t_1 t_2 \dots t_s$ отображения кубической системы также являются кубическими.

Группы G_D^n, порожденные операторами D_t^n, $t \neq 0$, симметрической динамической системы D большого обхвата (большого цикленного индикатора), образуют семейство подгрупп группы Кремоны $C(K^n)$. В случае двудольной динамической системы D возникают группы преобразований ${}^1G_D^n$ и ${}^2G_D^n$ многообразия P_nUL_n, порожденные $D^n t_1 t_2 \dots t_s$, действующие на P_n и L_n соответственно.

Простые графы и теоремы существования. Элементарные сведения о простых графах приведены в [8]. Напомним, что под обхватом простого графа понимают минимальную длину его цикла. Граф называется регулярным, если каждая его вершина имеет одинаковое количество соседей. Под размером $e(G)$ графа G понимают число его ребер.

Говорят, что бесконечное семейство графов G_i порядка v_i имеет суперлинейный размер если $e(G_i) = O(v_i^t)$, где $t > 1$.

Последовательность простых регулярных графов G_i возрастающего порядка v_i степени k_i и обхвата g_i называется семейством графов большого обхвата, если существует константа c такая, что $g_i > c \log k_i(v_i)$.

Существование таких семейств было установлено П. Эрдешем в конце 50-х годов XX ст. с помощью широко известного вероятностного метода. Известны две конструкции семейств связных графов большого обхвата и суперлинейного размера (графы Кэли, являющиеся графами Рамануджана [6, 7] и заданные уравнениями графы $CD(n,q)$) [8].

Цикловым показателем вершины простого графа называют минимальную длину проходящего через нее цикла. Цикловым показателем $h(G)$ графа G называют максимальное значение цикловых показателей его вершин.

Последовательность простых k_i регулярных графов возрастающего порядка и циклового показателя h_i называется семейством графов большого циклового показателя, если существует константа c, такая, что $h_i > c \log k_i(v_i)$. Существование такого семейства максимально возможного суперлинейного размера $e(v_i) \Leftrightarrow cv^{1+hi/2}$ установлено в [4].

Пусть D_t^n, $t \in K$, — двудольная симметрическая динамическая система большого обхвата (или циклового показателя). Рассмотрим простой двудольный граф $\Gamma_D^n(K)$ с долями P_n (множество точек) и L_n (множество прямых), такой, что инцидентность точки p и прямой l определяется условием: существует $t \in K$, такой, что $D_t^n(p) = l$.

Если кольцо K — конечно и $k = K$, то граф $\Gamma_D^n(K)$ имеет порядок $2k^n$ и степень k. Из определения двудольной симметричной динамической системы $D(K)$ большого обхва-

та (большого цикленного показателя) вытекает, что последовательность графов большого обхвата $\Gamma_D^n(K)$ является семейством графов большого обхвата (большого циклового показателя).

Пусть теперь D — симметрическая динамическая система большого обхвата (большого циклового показателя) над кольцом K. Однопараметрическому семейству D_t^n преобразований свободного модуля K^n сопоставим граф $\Gamma_D^n(K)$ с множеством вершин K^n, соответствующем симметричному бинарному отношению: $xIy \Leftrightarrow$ существует $t \in K$-$\{0\}$, такое, что $D^n t(x) = y$.

Очевидно, что в случае, когда кольцо K является полем, последовательность графов $\Gamma_D^n(K)$ образует семейство графов большого обхвата.

Введенные выше двудольные графы имеют регулярную раскраску ребер: ребро (x, y), $x \in P_n$, $y \in L_n$, окрашено в цвет t тогда и только тогда, когда $D^n t(x) = y$.

Теорема 1. *Для произвольного коммутативного кольца K существует*

1) двудольная кубическая динамическая система большого обхвата со скоростью роста больше или равно 1/2;

2) кубическая динамическая система большого обхвата со скоростью роста больше или равно 1/4;

3) двудольная кубическая динамическая система большого цикленного показателя со скоростью роста больше или равно 1;

4) кубическая динамическая система большого цикленного показателя со скоростью роста больше или равно 1/2.

Лемма 1. *Пусть $D(K)$ — двудольная симметрическая динамическая система большого обхвата (циклового показателя) над коммутативным кольцом большого обхвата (циклового показателя) над коммутативным кольцом характеристики больше или равно 2. Тогда отображения $D'^n_t = D^n_t D^n_t$, $t \geqslant 0$ образуют динамическую систему большого обхвата (циклового показателя, соответственно).*

Если скорость роста для $D(K)$ превышает c, то скорость роста для $D'(K)$ превышает $c/2$. Будем говорить, что двудольная динамическая система большого обхвата имеет полярность n, если существует автоморфизм n графа $\Gamma_D^n(K)$, такой, что $n^2 = e$, $x \in P_n \Rightarrow$ $\Rightarrow n(x) \in L_n$, $x \in L_n \Rightarrow n(x) \in P_n$, переводящий ребро x, y цвета t ребро цвета t'.

Лемма 2. *Пусть $D(K)$ — двудольная симметрическая система большого обхвата с полярностью n, имеющая скорость c. Тогда отображения $D'^n = D^n tn$ образуют симметрическую динамическую систему большого обхвата со скоростью, превышающей $c/2$.*

Пусть $D(K)$ — двудольная симметрическая динамическая система большого обхвата (циклового показателя) на последовательности многообразий $P_n U L_n$. Рассмотрим последовательность $P'_n U L'_n$, где P'_n и L'_n изоморфны свободному модулю K^{n+1}. Произвольный элемент $P'_n(L'_n)$ отождествим с парой $((p), D^n t(p))$, $p \in Pn$, $t \in K([[l], D^n t(l)]$, $l \in L_n$, $t \in K$, соответственно).

Рассмотрим двудольный граф с долями P'_n и L'_n, соответствующий отображению $D'^{n+1}t$, заданному соотношениями $D'^{n+1}t'((p), D^n t(p)) = [D^n t(p), D^n t' - t(D^n t(p))]$; $D'^{n+1}t'([l], D^n t[l]) = [D^n t(l)), D^n t' - t(D^n t(l))]$.

Лемма 3. *Отображения $D'^{n+1}t$ на многообразиях $K^{n+1}UK^{n+1}$ образуют двудольную динамическую систему $D'(K)$.*

Пусть n является полярностью двудольной симметрической динамической системы большого обхвата (циклового показателя). Тогда естественное действие n на $K^{n+1}UK^{n+1}$, опре-

деленное соотношениями $n((p), D^n t(p)) = (n(p), n(D^n t(p)),\ n([l], D^n t[p]) = (n[l], n(D^n t[l])$, является полярностью системы $D'(K)$.

Лемма 4. *Пусть n является полярностью двудольной динамической системы $D(K)$ большого обхвата, определенной на последовательности многообразий $M_n(K)UM_n(K)$. Тогда отображения $D'^n_t = D^n_t n$ определяют динамическую систему на последовательности многообразий $Mn(K)$.*

Лемма 5. *Пусть $D(K)$ — двудольная симметрическая динамическая система $C(D^n_t)^{-1} = D^n_{-t}$ со скоростью роста c, определенная над полем K, характеристики, отличной от 2.*

Тогда семейство операторов $D^n_t D^n_t$, $t \geqslant 0$ определяет симметрическую динамическую систему со скоростью роста не меньше, чем $c/2$.

Лемма 6. *Пусть $D(K)$ — двудольная симметрическая динамическая система с $(D^n_t)^{-1} = D^n_{-t}$ со скоростью роста c, определенная над полем K. Тогда семейство операторов $D'^n_t = D^n_o D^n t D^n_o$ также образует двудольную динамическую систему с той же скоростью роста, что и $D(K)$.*

Конструктивные примеры. Пусть K — конечное коммутативное кольцо. Рассмотрим двудольный граф $A(n, K)$, определенный на множестве точек $P = K^n$ и прямых $L = K^n$ через отношение инцидентности I: $x\,I\,y$ для $x = (x_1, x_2, \ldots, x_n)$ из P и $y = [y_1, y_2, \ldots, y_n]$ из L тогда и только тогда, когда выполняются соотношения $x_1 - y_1 = y_1 x_1$, $x_2 - y_2 = x_1 y_2$, $x_3 - y_3 = y_1 x_2$, $x_4 - y_4 = x_1 y_3$, $\ldots$, $x_n - y_n = x_1 y_{n-1}$ — при четном n и $x_n - y_n = y_1 x_{n-1}$ — при нечетном значении n. Круглые и квадратные скобки позволяют различать точки и прямые. Определим цвет точки $(x_1, x_2, \ldots, x_n)$ и прямой $[y_1, y_2, \ldots, y_n]$ как значения первых координат x_1 и y_1 этих векторов. Определенное выше семейство графов было введено в [9]. Его применения в криптографии и теории кодирования рассматривались в [10, 11].

Теорема 2. *Пусть $DA^n t(x)$ — оператор вычисления соседа вершины x в графе $A(n, K)$, тогда семейство отображений DA^n_t образует двудольную симметрическую динамическую систему с большим цикленным показателем, удовлетворяющую условию 3 теоремы 1.*

Рассмотрим бесконечный двудольный граф $D(K)$, определенный на множестве P точек $x = (x_1, x_2, x_3, x'_3, \ldots, x_n, x'_n, \ldots)$ и множестве L прямых $y = [y_1, y_2, y_3, y'_3, \ldots, y_n,\ y'_n, \ldots]$ через отношение инцидентности I: $x\,I\,y$ для x из P и y из L тогда и только тогда, когда выполняются соотношения $x_2 - y_2 = y_1 x_1$, $x_3 - y_3 = x_1 y_2$, $x_4 - y_4 = y_1 x_3$, $x_5 - y_5 = x_1 y_4$, $\ldots$, $x_n - y_n = x_1 y_{n-1}$ — при нечетном n и $x_n - y_n = y_1 x_{n-1}$ — при четном значении n, вместе с соотношениями $x'_3 - y'_3 = y_1 x_2$, $x'_4 - y'_4 = x_1 y'_3$, $x_5 - y_5 = y_1 x'_4$, $\ldots$, $x'_n - y'_n = y_1 x'_{n-1}$ — при нечетном n и $x'_n - y'_n = x_1 y_{n-1}$ — при четном значении n.

Рассмотрим также двудольный граф $D(n, K)$, определенный на множестве точек $Pn = = K^n$ и прямых $L_n = K^n$ следующим образом: векторы x_n иy_n из P_n и L_n, соответственно, отождествляются с проекциями $x \in P$ и $y \in L$ на первые n координат, x_n и y_n связаны ребром тогда и только тогда, когда выполняются первые $n-1$ соотношений, определяющих инцидентность векторов x и y. Для случая $K = F_q$ семейство графов $D(n, K) = D(n, q)$ было определено в [12]. Индуцированные подграфы $CD(n, q)$ графов $D(n, q)$ были введены в [8], где изучались экстремальные свойства подграфов. В общем случае графы $D(n, K)$ и $CD(n, K)$ впервые введены в [13]. Наиболее общие результаты о связности $CD(n, K)$ получены в [14], динамические системы, соответствующие этим семействам графов, впервые рассматривались в [9]. Если K является коммутативным кольцом характеристики, отличной от 2, то граф $CD(n, K)$ просто совпадает со связной компонентой $D(n, q)$. Множества P_n

и L_n точек и прямых графа $D(n,q)$ отождествляются с K^t, где $t = [3/4n] + 1$ для $n = 0, 2, 3 \mod 4$ и $t = [3/4n] + 2$ для $n = 1 \mod 4$.

Теорема 3. *Пусть $D^n t(x)$ — оператор вычисления соседа вершины x в графе $D(n,K)$, $CD^n t(x)$ — его ограничение на множество вершин графа $CD(n,K)$. Тогда семейства отображений D_t^n и CD_t^n образуют двудольные симметрические динамические системы $D(K)$ и $CD(K)$ большого обхвата, удовлетворяющие условиям 1 и 2 теоремы 1, соответственно.*

Из этого утверждения следуют полученные ранее результаты, опубликованные в [9, 15]. Двудольные симметрические динамические последовательности $D^{2n}(K)$ и $CD^{2n}(K)$ систем $D(K)$ и $CD(K)$, соответственно, большого обхвата теоремы 3 имеют полярность n и скорость роста больше или равно $1/2$ и больше или равно $2/3$. Применение конструкции леммы 3 к этим последовательностям определяет кубическую симметрическую динамическую последовательность $D1^{2n}(K)$ большого обхвата со скоростью роста больше или равно $1/4$ и симметричесую последовательность $CD1^{2n}(K)$ со скоростью роста больше или равно $1/3$.

Семейства графов $\Gamma_1^{2n}(K)$ и $C\Gamma_1^{2n}(K)$, соответствующие этим последовательностям, при $K = Fq$ являются семействами $q-1$ регулярных графов большого обхвата (см. [9]).

Пусть $D(K)$ и $CD(K)$ — двудольная симметрическая динамическая система большого обхвата теоремы 3, определенная над коммутативным кольцом K. Отображения D_{2t}^{n+1} на многообразиях $K^{n+1}UK^{n+1}$, полученные применением построения леммы 4, образуют двудольную кубическую динамическую систему $D_2(K)$ большого обхвата со скоростью больше или равно $1/2$. А отображения $CD_2^{n+1}t$ образуют двудольную динамическую систему $CD2(K)$. Полярность n двудольной симметрической динамической последовательности $D^{2n}(K)(CD^{2n}(K))$ индуцирует полярность двудольной динамической последовательности $D_2^{2n+1}(K)$ ($CD_2^{2n+1}(K)$, соответственно) большого обхвата. Конструкция леммы 5 определяет динамические последовательности $D_3^{2n+1}(K)$ и $CD_3^{2n+1}(K)$ большого обхвата.

Приведенные выше примеры динамических систем определены над произвольным коммутативным кольцом. Пусть $CD(F)$ и $DA(F)$ — введенные выше двудольные симметрические динамические системы большого обхвата и цикленного показателя над полем F характеристики больше или равно 2.

Тогда отображения $CD'^n t = CD^n t CD^n t$, t — отлично от 0 и $DA'^n t = DA^n t DA^n t$, t — отлично от 0, согласно лемме 1, образуют симметрические динамические системы $CD_4(F)$ и $DA_1(F)$ большого обхвата и циклового показателя соответственно. Обозначим через $\Gamma_4(F)$ и $\Gamma A_1(F)$ семейства простых графов динамических систем $CD_4(F)$ и $DA_1(F)$. Конструкции леммы 2 и леммы 6, примененные к двудольным симметрическим динамическим системам $CD(F)$ и $DA(F)$, определяют новые двудольные симметрические динамические системы $\Gamma_5(F)$ и $\Gamma A_2(F)$ и $\Gamma_6(F)$ и $\Gamma A_3(F)$ соответственно.

Теорема 6. *Семейства графов $\Gamma_4(Fq)$, $\operatorname{char} Fq \geqslant 3$, $\Gamma_5(Fq)$, $\Gamma_6(Fq)$, зависящие от неограниченного параметра q, являются семействами графов большого обхвата, суперлинейного размера без реберно-транзитивной группы автоморфизмов.*

Семейства графов $\Gamma A_1(Fq)$, $\operatorname{char} Fq \geqslant 3$, $\Gamma A_2(Fq)$, $\Gamma A_3(Fq)$ образуют новые суперлинейные семейства простых графов с большим цикловым показателем.

1. *Ding J., Gower J. E., Schmidt D. S.* Multivariate public key cryptosystems. – Berlin: Springer, 2006. – 260 p.
2. *Ustimenko V.* Graphs with special arcs and cryptography // Acta Appl. Math. – 2002. – No 2. – P. 117–153.

3. *Ustimenko V.* Maximality of affine group and hidden graph cryptosystems // J. Algebra Discrete Math. – 2005. – **1**. – P. 133–150.
4. *Устименко В. А.* Об экстремальной теории графов и символьных вычислениях // Доп. НАН України. – 2013. – № 2. – С. 42–49.
5. *Bollobas B.* Extremal graph theory. – London: Academic Press, 1978. – 320 p.
6. *Margulis G. A.* Explicit construction of graphs without short cycles and low density codes // Combinatorica. – 1982. – **2**. – P. 71–78.
7. *Lubotsky A., Philips R., Sarnak P.* Ramanujan graphs // J. Comb. Theory. – 1989. – **115**, No 2. – P. 62–89.
8. *Lazebnik F., Ustimenko V. A., Woldar A. J.* New series of dense graphs of high girth // Bull (New Series) of AMS. – 1995. – **32**, No 1. – P. 73–79.
9. *Ustimenko V.* Linguistic Dynamical systems, graphs of large girth and cryptography // J. Math. Sci. – 2007. – **140**, No 3. – P. 412–434.
10. *Romanczuk U., Ustimenko V.* On the key exchange with new cubical maps based on graphs // Annales UMCS Informatica. – 2011. – **4**, No 11. – P. 11–19.
11. *Polak M., Ustimenko V.* On LDPC codes corresponding to infinite family of graphs $A(n, K)$. – Proceedings of Federated Conference on Computer Science and Informations Systems. – September 9–12, 2012. – Wroclaw, Poland. – P. 567–570.
12. *Lazebnik F., Ustimenko V.* Some algebraic constractions of dense graphs of large girth and of large size, DIMACS series // Discrete Mathematics and Theoret. Computer Science. – 1993. – **10**. – P. 75–93.
13. *Ustimenko V.* Coordinatisation of trees and their quotients // Voronoj's Impact on Modern Science. – 1998. – **2**. – P. 125–152.
14. *Ustimenko V.* Algebraic groups and small world graphs of high girth // Albanian J. Math. – 2009. – **3**, No 1. – P. 25–33.
15. *Wroblewska A.* On some applications of graph based public key // Ibid. – 2008. – **2**, No 3. – P. 229–234.

Институт телекоммуникаций
и глобального информационного пространства
НАН Украины, Киев
Университет Марии Кюри–Склодовской, Люблин

Поступило в редакцию 24.12.2012

В. О. Устименко

Про K-теорію динамічних систем, що відповідають графам, та її застосування

Визначаються деякі класи залежних від часу дискретних динамічних систем. Означення мотивовані проблемами криптографії, що базується на поліноміальних перетвореннях від багатьох змінних, зокрема пошуком циклічних груп поліноміальних перетворень необмеженого порядку, утворених перетвореннями степені не більше, ніж 3. Існування визначених аксіомами дискретних динамічних систем доводиться методами конструктивної екстремальної теорії графів. Деякі динамічні системи визначаються за побудовою нових прикладів сімей графів великого обхвату суперлінійного розміру. Зокрема наводиться конструкція такої сім'ї графів без реберно транзитивної групи автоморфізмів. Побудовано також нові приклади сімей графів з великим цикловим показником.

V. A. Ustimenko

On the K-theory of graph-based dynamical systems and its application

Special classes of time-dependent discrete dynamical systems are defined. The definitions are motivated by problems of multivariate cryptography, in particular, by the search for sequences of cyclic groups of polynomial transformations in the increasing number of variables of unbounded order formed by elements of a degree of at most 3. The existence of the dynamical systems defined by axioms is proven by methods of the constructive extremal graph theory. Some dynamical systems are defined by new explicit constructions of the families of simple graphs of large girth with superlinear size. We introduce the construction of such family without edge transitive automorphism group. Some new families of graphs with large cycle indicator are introduced.