УДК 519.176,519.157.2

В. А. Устименко

Об экстремальной теории графов и символьных вычислениях

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

Минимальную длину цикла, проходящего через выбранную вершину простого графа, назовем цикловым индикатором вершины. Цикловой индикатор графа определим как наибольшее значение цикловых индикаторов его вершин. Регулярный граф называется графом с иррегулярным цикловим индикатором, если его цикловой индикатор отличается от обхвата. В работе приводится полное решение оптимизационной задачи вычисления максимального размера $e = e(v)$ для графов заданного порядка v с цикловым индикатором, превышающим выбранный параметр d, $d > 2$. Рассматривается задача нахождения наименьшего порядка для k-регулярного графа с цикловим индикатором d. Приводится алгебраическая конструкция бесконечной семьи регулярных графов заданной степени с возрастающим иррегулярным цикловим индикатором асимптотически максимального размера. Построенная бесконечная последовательность графов заданной степени p^s, где p — произвольное нечетное простое, а s — произвольное натуральное число, образует семью графов малого мира. Обсуждаются криптографические применения этой конструкции.

Постановка задач. Будем предполагать, что все рассматриваемые графы являются простыми. Они являются графами симметричных бинарных отношений и не содержат петель. Будем использовать определения и обозначения [1]. В частности, $V(G)$ и $E(G)$ обозначают множества вершин и ребер графа G. Число $|V(G)|$ будем называть порядком G, а параметр $|E(G)|$ — *размером* G. Цепь в G будем называть *простой*, если все ее вершины различны. Длина цепи совпадает с числом принадлежащих ей ребер. Мы не будем различать граф G и соответствующее ему антирефлексивное бинарное отношение на множестве $V(G)$.

Обхватом графа, обозначаемым символом $g = g(G)$, будем называть длину кратчайшего цикла в G. Классическая экстремальная теория графов изучает максимальный размер $e(v, F_i)$, $i = 1, 2, \ldots, m$, графа порядка v, не содержащего подграфы, изоморфные графам из заданного списка F_i, $i = 1, 2, \ldots, m$. Параметр v рассматривается как переменная, при этом употребляются следующие стандартные обозначения.

Пусть f и g — действительные функции, определенные на открытом интервале от $a > 0$ до бесконечности:

а) $f(x) <=> g(x)$, если $f(x)/g(x)$ стремится к 1 при x, стремящемся к бесконечности;

б) $f(x) = o(g(x))$, если $f(x)/g(x)$ стремится к 0 при x стремится к бесконечности;

в) $f(x) = O(g(x))$, если существуют C и x_0, такие, что $|f(x)| < C|g(x)|$ для всех $x > x_0$;

г) $f(x) = \Omega(g(x))$, если существует постоянная $c > 0$ и неограниченная последовательность x_i, $i = 1, 2, \ldots$, такие, что $|f(x_i)| > c|g(x)_i)|$ для всех i.

Пусть C_n означает цикл длиной n. Известная теорема Эрдеша о четном цикле утверждает, что максимальный размер $\mathrm{ex}(v, C_{2k})$ графа на v вершинах, не содержащего цикла C_{2k}, равен $O(v^{1+1/k})$. Доказательство этого утверждения и его обобщений можно найти в [2, 3]

(см. также дальнейшие ссылки). Оно было получено вероятностным методом Эрдеша. Очевидно, что этот результат устанавливает верхнюю оценку для $\mathrm{ex}(v, C_{2k})$. Известно, что при $k = 2$, 3 и 5 (см. [4, 5] для $k = 2$ и [6] для $k = 3$, 5) приведенная выше оценка точна, т. е. $\mathrm{ex}(v, C_{2k}) = \Omega(v^{1+1/k})$. Эквивалентность $\mathrm{ex}(v, C_4) <=> 1/2v^{3/2}$ была установлена в [7] и [4]. Наилучшие известные оценки снизу для $k = 3$ и $k = 5$ найдены в [8, 9], где было установлено, что $\mathrm{ex}(v, C_6)$ превышает $1/2v^{4/3} + o(v^{4/3})$ и $\mathrm{ex}(v, C_{10})$ не меньше чем $4/5^{6/5}v^{6/5}$.

Вопрос о точности верхней оценки, приведенной в теореме о четном цикле при k, отличном от 2, 3, 5, был сформулирован еще в начале 60-х. Он остается открытым и в наши дни.

Исследования максимального размера $\mathrm{ex}(v, C_3, C_4, \ldots, C_{2n})$ графа на v вершинах без циклов C_3, C_4, …, C_{2n}, т. е. графов обхвата $> 2n$, были мотивированы как их приложениями к теории конечных геометрий и структур инцидентности, так и практическими применениями в телефонных сетях. Следствием теоремы о четном цикле является неравенство $\mathrm{ex}(v, C_3, C_4, \ldots, C_{2n}) = O(v^{1+1/n})$.

Ниже приведены более сильные оценки сверху

$$\mathrm{ex}(v, C_3, C_4, \ldots, C_{2n}, C_{2n+1}) < \left(\frac{1}{2}\right)^{1+1/n} v^{1+1/n} + o(v^{1+1/n}), \tag{1}$$

$$\mathrm{ex}(v, C_3, C_4, \ldots, C_{2n}) < \frac{1}{2}v^{1+1/n} + o(v^{1+1/n}). \tag{2}$$

Неравенство (1) было установлено в [5] для всех $k > 1$. Верхняя оценка (2) может быть получена подобными вероятностными методами (см., например, [10]). Так же, как и в случае $\mathrm{ex}(v, C_{2n})$, вопрос об асимптотической точности оценок (1) и (2) решен только для $n = 2, 3, 5$.

Впервые общая оценка снизу вида

$$\mathrm{ex}(v, C3, C4, \ldots, Cn) < \Omega(v^{1+1/cn}), \tag{3}$$

где c является постоянной $< 1/2$, была получена Эрдешем в конце 50-х годов при изучении *семейств графов большого обхвата*, т. е. бесконечных семейств простых регулярных графов G_i, $i = 1, 2, \ldots$, степени k, порядка v_i таких, что $g(G_i)$ превышает $c \log_k(vi)$, для не зависимой от i константы c. Эрдеш доказал существование такого семейства для произвольной ограниченной степени k и константы $c = 1/4$ своим вероятностным методом. Всего несколько конструктивных примеров семейств графов большого обхвата произвольно большой, но ограниченной степени, известно: семья графов Кэли, определенная в работе Г. А. Маргулиса [11] и детально исследованная в дальнейшем в [12], семейство алгебраических графов $CD(n, q)$ [13] и его модификация с помощью автоморфизма порядка 2 предложена в [14]. Напомним, что $\mathrm{ex}(v, C_{2k})$ не может быть меньше, чем $\mathrm{ex}(v, C_3, C_4, \ldots, C_{2k+1})$.

Лучшая известная оценка снизу для максимального размера графа порядка v обхвата $> 2k + 1$, где k отлично от 2, 3, 5, была получена в [13]:

$$\mathrm{ex}(v, C_3, C_4, \ldots, C_{2k+1}) = \Omega(v^{1+2/(3k-3+e)}).$$

Здесь $e = 0$, если k нечетно, и $e = 1$ — для четного k.

Пусть G — простой граф и $\mathrm{Cind}(x)$ — минимальная длина цикла, содержащего вершину x графа G, обозначим через $\mathrm{Cind}(G)$ максимальное значение параметра $\mathrm{Cind}(x)$ по всем x из множества $V(G)$. Параметр $\mathrm{Cind}(G)$ будем называть цикловым индикатором графа G. Работа посвящена исследованию следующих вопросов.

1. Каково максимальное значение $e(v,n)$, $n>3$ для размера (количество ребер) графа G на v вершинах цикловым индикатором $\mathrm{Cind}(G)>n$?

Напомним, что простой граф G является регулярным (k-регулярным) если его произвольная вершина имеет в точности k соседей. Далее будем полагать, что все рассматриваемые графы являются регулярными.

2. Каково минимальное значение порядка $o(k,n)$, $n>3$, для k-регулярного графа G с цикловым индикатором $\mathrm{Cind}(G)=n$?

Определим *семейство графов с большим цикловым индикатором* как бесконечное семейство простых регулярных графов G_i степени k, порядка v_i, таких, что $\mathrm{Cind}(G_i)$ превышает $c\log_k(v_i)$ для независимой положительной константы c.

В следующей секции будет показано, что наибольшая возможная константа c в неравенстве, определяющем семейство графов с цикловым индикатором, равняется двум. Такую последовательность графов G_i, удовлетворяющих условию неравенства $\mathrm{Cind}(G_i)$ и $g(G_i)$, будем называть*семейством графов с большим иррегулярным цикловым индикатором.*

Термин иррегулярный употреблен в связи с тем, что цикловой индикатор вершины не является постоянным для всех вершин. Очевидно, что представители G_i семьи графов с переменным цикловым показателем не могут быть вершинно транзитивными, т. е. группа симметрий G_i не может действовать транзитивно на множестве $V(G_i)$. Напомним, что расстояние между вершинами графа определяется как минимальная длина пути между ними. С другой стороны, семья вершинно-транзитивных графов с большим цикловым индикатором будет семьей графов большого обхвата.

Диаметром графа называется максимальное расстояние между его вершинами. *Семейство графов малого мира* определяется как бесконечное семейство простых регулярных графов G_i степени k, порядка v_i, таких, что диаметр $d(G_i)$ для G_i превышает $c\log_k(v_i)$ для независимой положительной константы c. Известна конструкция семьи графов малого мира фиксированной степени, которая является одновременно и семьей графов с большим цикловым показателем с константой $c=4/3$ (см. [11, 12]). Ввиду ее вершинной транзитивности она будет и семьей большого обхвата.

Ниже приводится конструкция семьи графов с иррегулярным цикловым индикатором с максимальной константой $c=2$, которая одновременно является семьей графов малого мира. Мы рассмотрим также криптографические приложения этой конструкции.

Точные оценки и конструкции семейств графов с большим цикловым индикатором.

Теорема 1.

$$e(v,2n+1)\Leftrightarrow\left(\frac{1}{2}\right)^{1+1/n}v^{1+1/n}+o(v^{1+1/n}). \tag{4}$$

Теорема 2.

$$\left(\frac{1}{2}\right)^{1+1/n}v^{1+1/n}<e(v,2n)<\frac{1}{2}v^{1+1/n}+o(v^{1+1/n}). \tag{5}$$

Замечание. Из верхних оценок теорем 4 и 5 следуют неравенства (1) и (2).

Лемма 1.

$$2(1+(k-1)+\cdots+(k-1)^n)<o(k,2n+2),$$

$$1+k(k-1)+k(k-1)^2+\cdots+k(k-1)^{(n-1)}<o(k,2n+1).$$

Доказательство. Пусть x — вершина с максимальным цикловым индикатором, равным $2n+2$ графа степени k. Рассмотрим вершину y, соседнюю с x, а также корневые деревья с корнями x и y глубиной n, не содержащие вершины y и x соответственно. Каждое из деревьев содержит $1+(k-1)+\cdots+(k-1)^n$ вершин, причем все они различны. Таким образом устанавливается нижняя оценка для $o(k, 2n+2)$.

Пусть теперь x — вершина с максимальным цикловым индикатором графа степени k с цикловым индикатором $2n+1$. Рассмотрим корневое дерево с корнем x глубины n. Его порядок равен $1+k(k-1)+k(k-1)^2+\cdots+k(k-1)^{(n-1)}$. Таким образом получается нижняя оценка для $o(k, 2n+1)$.

Приведенная выше лемма несколько обобщает известную лемму Тата (Tutte), устанавливающую нижнюю границу для порядка k — регулярного графа заданного обхвата.

Пусть F_q — конечное поле порядка q, являющегося степенью простого числа. Рассмотрим двудольный граф $A(n, F_q) = A(n, q)$, определенный на множестве точек $P = F_q^n$ и прямых $L = F_q^n$ 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 $y_2 - x_2 = y_1x_1$, $y_3 - x_3 = x_1y_2$, $y_4 - x_4 = y_1x_3$, $y_5 - x_5 = x_1y_4$, $\ldots$, $y_n - x_n = x_1y_{n-1}$ при нечетном n и $y_n - x_n = y_1x_{n-1}$ — при нечетном значении n, $n>1$. Круглые и квадратные скобки позволяют различать точки и прямые.

Лемма 2. *Пусть* $u_1 = [0, 0, \ldots, 0]$, $u_2 = (a_1, 0, \ldots, 0)$, $u_3 = [b_1, -a_1b_1, a_1^2b_1, 0, \ldots, 0]$, $\ldots$, u_n *— путь в графе* $A(n, q)$ *с началом в нулевой прямой длиной* n. *Тогда последняя координата* z_n *последней вершины пути* $u_n = (z_1, z_2, \ldots, z_n)$ *равна* $-a_1b_1(a_1-a_2)(b_1-b_2)\cdots(b_{k-1}-b_k)(a_k-a_{k+1})$ *при нечетном значении* $n = 2k+1$ *и* $a_1b_1(a_1-a_2)(b_1-b_2)\cdots(a_{k-1}-a_k)(b_{k-1}-b_k)$ *при четном значении* $n = 2k$ *соответственно.*

Лемма 3. *Пусть* $w_1 = (0, 0, \ldots, 0)$, $w_2 = [c_1, 0, \ldots, 0]$, $w_3 = (d_1, c_1d_1, -d_1^2(c_1 - c_2, 0, \ldots)$, $\ldots$, w_n. *Тогда две последние координаты конечного вектора (точки или прямой)* w_n *равны* $c_{2k}d_{2k-1}(c_1-c_2)(d_1-d_2)\cdots(c_{k-1}-c_k)(d_{k-1}-d_k, 0)$ *при нечетном* $n = 2k+1$ *и* $(d_k-d_{k-1})^2(c_1-c_2)(d_1-d_2)\cdots(d_{k-2}-d_{k-1})(c_{k-1}-c_k, 0)$ *при четном* $n = 2k$ *соответственно.*

Непосредственно из определения вытекает, что графы $A(2, q)$ и $A(3, q)$ изоморфны известным графам $D(2, q)$ и $D(3, q)$ обхвата >4 и >6 соответственно.

Лемма 4. *Пусть* L_t *— преобразование множества вершин графа* $A(n, q)$, *такое, что* L_t *не изменяет нечетных координат точки* x *из* P *и изменяет* x_{2i} *на* $x_{2i} + tx_{2i-1}$, L_ty_1 *на* $y_1 + t$ *и оставляет другие компоненты без изменения. Тогда* L_t *является автоморфизмом* $A(n, q)$.

Теорема 3. *Цикловой индикатор графа* $A(n, q)$ *превышает* $2n$.

Доказательство. Воспользуемся индукцией по n. База индукции обоснована справедливостью утверждения при $n = 2$ и $n = 3$. Предположение индукции равносильно неравенству $\mathrm{Cind}(A(n-1, q)) > 2n-2$. Ввиду следствия из леммы 1 $\mathrm{Cind}(A(n, q))$ больше или равен $2n-2$. Исследуем цикловой показатель точки $(0, 0, \ldots, 0)$ графа $A(n, q)$. Соседом этой точки является прямая вида $u = [a, 0, 0, \ldots, 0]$.

Заметим, что автоморфизм L_t оставляет точку $(0, 0, \ldots, 0)$ неподвижной при любом t из F_q. Преобразование L_{-a} переводит u в прямую $[0, 0, \ldots, 0]$. Таким образом, без потери общности можем полагать, что цикл, содержащий точку $(0, 0, \ldots, 0)$, содержит и прямую $[0, 0, \ldots, 0]$. Цикл длиной n через нулевое ребро образуется двумя путями, описанными в леммах 2 и 3: первый из них содержит $u_1 = [0, 0, \ldots, 0]$, $u_2 = (a_1, 0, \ldots, 0)$, $u_3 = [b_1, -a_1b_1, a_1^2b_1, 0, \ldots, 0]$, $\ldots$, u_n, второй образован вершинами $w_1 = (0, 0, \ldots, 0)$, $w_2 = [c_1, 0, \ldots, 0]$, $w_3 = (d_1, c_1d_1, -d_1^2(c_1 - c_2), 0, \ldots, 0)$, $\ldots$, w_n. Для существования цикла необ-

ходимо равенство $w_n = u_n$ при условии, что все остальные вершины в приведенном выше списке различны и отличны от w_n. Различие вершин равносильно отличию от нуля параметров a_1, $a_i - a_{i+1}$, b_i, c_1, $c_i - c_{i+1}$, $d_i - d_{i+1}$ при $i{>}0$. Неравенства для a_i и b_i гарантируют отличие от нуля последней координаты вектора u_n, описанной в лемме 2. Последняя же координата вектора w_n, согласно лемме 3, равна нулю. Таким образом, условие равенства векторов w_n и u_n невыполнимо, что и означает $A(n,q) > 2n$. Теорема доказана.

Граф $A(n,q)$ является двудольным, поэтому он не содержит нечетных циклов. Порядок графа $2q^n$ не превышает $2(1+(q-1)+\cdots+(q-1)^n)$ при $q > 2$. Таким образом из приведенной выше теоремы и леммы 1 получаем следующие утверждение.

Следствие 1. *При $q > 2$ цикловой индикатор графа $A(n,q)$ равен $2n+2$.*

Пусть $p(k)$ — наименьшая степень простого числа, превышающего k.

Следствие 2. *Последовательность $A(n,q)$, $n = 2,3,\ldots$, при каждом q образует семейство графов с большим цикловым индикатором со скоростью роста $c = 2$.*

Пусть $p(k)$ — наименьшая степень простого числа, превышающего k.

Лемма 5.

$$2(1 + (k-1) + (k-1)^2 + \cdots + (k-1)^n) < o(k, 2n+2) < 2kp(k)^{n-1}.$$

Теорема 4. *Последовательность $A(n,q)$, $n = 2,3,\ldots$, при каждой нечетной степени q простого числа образует семейство графов малого мира с большим иррегулярным цикловым индикатором.*

Рассмотрим естественный гомоморфизм h_n графа $A(n,q)$ на $A(n-1,q)$, соответствующий операции стирания последних координат точек и прямых

$$h_n((x_1, x_2, \ldots, x_n)) = (x_1, x_2, \ldots, x_{n-1}), \qquad h_n([y_1, y_2, \ldots, y_n]) = [y_1, y_2, \ldots, y_{n-1}].$$

Последовательность гомоморфизмов определяет проективный предел $\lim A(n,q)$ при n, стремящемся к бесконечности.

Теорема 5. *Проективным пределом последовательности графов $A(n,q)$ является q-регулярное дерево T_q.*

Напомним, что семья k-регулярных графов G_i называется семьей экспандеров, если второе собственное значение $\lambda_1(G_i)$ каждого из графов отграничено от k.

Теорема 6. *Графы $A(n,q)$ образуют семью экспандеров, при этом $\lambda_1(A(n,q))$ не превышает $2q^{1/2}$.*

Автоматы, определенные графами семейства $A(n,q)$. Графы $A(n,q)$ были определены в [14] как гомоморфные образы графов $D(n,q)$. В этой же публикации вводится цвет вершины (точки или прямой) как значение первой координаты вектора вершины. Таким образом, цвета являются элементами конечного поля F_q. В графе $A(n,q)$ каждая вершина v имеет единственного соседа заданного цвета. Рассмотрим биективное отображение Dt из множества вершин графа $A(n,q)$, переводящее точку $x = (x_1, x_2, \ldots, x_n)$ в ее соседа цвета $x_1 + t$, где t принадлежит полю F_q, и переводящее прямую $y = [y_1, y_2, \ldots, y_n]$ в соседнюю с ней точку цвета $y_1 + t$. Простой путь длиной s в графе с началом в вершине v может быть представлен как последовательность вершин $x_0 = v$, $x_1 = Dt_1(x_0)$, $x_2 = Dt_2(x_1)$, $\ldots$, $x_s = Dt_s(x_{s-1})$, где последовательность $t = t_1$, t_2, $\ldots$, t_s удовлетворяет условию t_i и $-t_{i-1}$ различны при $i = 1,2,\ldots,s$. Пусть Dt — отображение, переводящее v в x_s. Заметим, что обратным к нему будет биекция Dt', где t' — последовательность $-t_s$, $-t_{s-1}$, $\ldots$, $-t_1$. Оказалось, что независимо от выбора

последовательности преобразование Dt является полиномиальным преобразованием вида $(x_1, x_2, \ldots, x_n) \to (f_1(x_1, x_2, \ldots, x_n), f_2(x_1, x_2, \ldots, x_n), \ldots, f_n(x_1, x_2, \ldots, x_n))$, где все многочлены $f_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$, являются кубическими.

Пометив ребро между соседними вершинами v_1 и v_2 разностью их цветов, получим конечный автомат с алфавитом F_q. Семью автоматов $A(n, q)$ можно использовать для кодирования "потенциально бесконечного текста" над F_q. Будем считать, что открытый текст x является элементом выбранной доли, например, P. Последовательность $t = t_1, t_2, \ldots, t_s$ цветов ребер простого пути в автомате, соответствующего вычислению функции $Dt(x)$, назовем несократимым пассвордом. На векторном пространстве F_q^n рассмотрим два обратимых аффинных преобразования L_i, $i = 1, 2$, вида $x \to xA_i + b_i$, где A_i является разреженной матрицей, а b_i — векторами вида $(b_1, b_2, \ldots, b_n)$. Напомним, что разреженность матрицы означает ее вычислимость за $O(n)$ шагов. Будем считать, что персональный ключ состоит из пар A_i, b_i, $i = 1, 2$, и несократимого пассворда $t = t_1$, $t_2, \ldots, t_s$. Кодирующее отображение E — композиция L_1, Dt и L_2, Обратным к нему будет отображение $L_2' Dt' L_1'$, где L_i' — обратные к L_i аффинные отображения, а t' — последовательность $-t_s$, $-t_{s-1}$, $\ldots$, $-t_1$. Кубическое преобразование E вычисляем с помощью одного из пакетов, реализующего символьные преобразования компьютерной алгебры. Результатом вычисления будет полиномиальное преобразование $G\colon (x_1, x_2, \ldots, x_n) \to (g_1(x_1, x_2, \ldots, x_n), g_2(x_1, x_2, \ldots, x_n), \ldots, g_n(x_1, x_2, \ldots, x_n))$, где все многочлены $g_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$, являются кубическими выражениями, записанными в виде списка упорядоченных мономов.

Список G будет служить публичным правилом (ключем), так что публичный пользовать может с его помощью кодировать информацию за не более чем $O(n^4)$ шагов. Хозяин ключа, имеющий информацию о семействе графов, и персональный ключ может осуществлять как кодирование, так и декодирование за время $O(n)$. Заметим, что он может фактически использовать генератор публичных ключей, меняя параметры n (длина потенциально бесконечного текста), s (длина несократимого пассворда), q (выбор алфавита). Отметим, что наилучший общий алгоритм нахождения обратного к G преобразования требует $3^{O(n)}$ шагов, независимо от того, использует ли он идеологию базиса Гребнера или альтернативные методы. Из определения семейства графов с большим цикловым показателем следует, что *при условии $s < n$ и фиксированных аффинных преобразованиях L_i, $i = 1, 2$, различным несократимым пассвордам соответствуют различные отображения G.*

Описанный выше симметрический алгоритм имеет самостоятельную ценность как потоковый алгоритм быстрого шифрования. Если q — нечетно, то из-за связности графа при фиксированных аффинных преобразованиях L_i, $i = 1, 2$, и переменных несократимых пассвордах произвольной длины кодирование обладает свойством транзитивности, т. е. *для произвольно выбранных открытых текстов (файлов одинакового размера) существует пассворд, такой, что соответствующее кодирующее отображение переводит первый текст во второй.*

Заметим, что для блоковых алгоритмов свойство транзитивности невозможно, так как открытый текст с периодичностью на блоках при любом кодировании переводится в новый периодичный текст. *Свойство графов малого мира гарантирует транзитивность даже при ограничении пространства пассвордов на множество слов длиной $O(n)$.* Кодирование при использовании таких ограниченных пассвордов осуществляется за $O(n^2)$ шагов.

Важный частный случай соответствует выбору обратного к L_1 афинного преобразования в качестве L_2. Для простоты предположим, что s четно. В этом случае порядок

отображения G совпадает с порядком Dt. Как вытекает из приведенных выше результатов, в этом случае

1) любая степень отображения G в симметрической группе $S(F_q^n)$ является либо кубическим отображением векторного пространства в себя, либо единицей;

2) если t_1+t_s отлично от нуля, то порядок преобразования G стремится к бесконечности при возрастании параметра n.

Свойства 1 и 2 мотивируют следующий протокол смены ключа. Корреспонденты А и Б используют публичное отображение G. Они секретно выбирают натуральные числа $K_{\text{а}}$ и $K_{\text{б}}$. После этого через открытый канал А посылает $G^{K a}$ корреспонденту Б. Пользователь Б в ответ высылает $G^{K\text{б}}$. После чего пользователи А и Б вычисляют независимо общий ключ F как $G^{K\text{б}}$ в степени Kа и G^{Ka} в степени $K_{\text{б}}$, соответственно. Пользователи могут использовать $F\colon (x_1, x_2, \ldots, x_n) \to (f_1(x_1, x_2, \ldots, x_n), f_2(x_1, x_2, \ldots, x_n), \ldots, f_n(x_1, x_2, \ldots, x_n))$ в форме массива лексикографически упорядоченных коэффициентов полиномов из правых частей $f_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$, или функции от этого массива. Примером может служить одномерный массив $(d/dx_1+d/dx_2+\cdots+d/dx_n)^3 f_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$ (см. [15]).

1. *Bollobas B.* Extremal graph theory. – London: Academic Press, 1978. – 440 p.
2. *Bondy J. A., Simonovits M.* Cycles of even length in graphs // J. Combin. Theory. Ser. B. – **16**. – 1974. – P. 87–105.
3. *Faudree W., Simonovits M.* On a class of degenerate extremal graph problems // Combinatorica. – **3** (**1**). – 1983. – P. 83–93.
4. *Erdos P., R'enyi A., S'oc V. T.* On a problem of graph theory // Studia. Sci. Math. Hungar. – **1**. – 1966. – P. 215–235.
5. *Erdos P., Simonovits M.* Compactness results in extremal graph theory // Combinatorica. – 1982. – **2** (**3**). – 1982. – P. 275–288.
6. *Benson C. T.* Minimal regular graphs of girth eight and twelve // Canad. J. Math.. – **18**. – 1966. – P. 1091–1094.
7. *Brown W. G.* On graphs that do not contain Thomsen graph // Canad. Math. Bull. **9**, No 3. – 1966. – P. 281–285.
8. *Lazebnik F., Ustimenko V. A., Woldar A. J.* Polarities and $2k$-cycle-free graphs // Discrete Mathematics. – **197/198**. – 1999. – P. 503–513.
9. *Lazebnik F., Ustimenko V. A., Woldar A. J.* Properties of certain families of $2k$-cycle free graphs // J. Combin. Theory. Ser. B. – **60**, No 2. – 1994. – P. 293–298.
10. *Ustimenko V.* On the cryptographical properties of extreme algebraic graphs / Algebraic Aspects of Digital Communications // NATO Science for Peace and Security. Ser. D: Information and Communication Security, IOS Press. – 2009. – **24**. – P. 256–281.
11. *Margulis G. A.* Explicit construction of graphs without short cycles and low density codes // Combinatorica. – **2**. – 1982. – P. 71–78.
12. *Lubotsky A. R., Philips R. P., Sarnak P.* Ramanujan graphs // J. Comb. Theory. – **115**, No 2. – 1989. – P. 62–89.
13. *Lazebnik F., Ustimenko V. A., Woldar A. J.* New series of dense graphs of high girth // Bull (New Series) of AMS. – **32**, No 1. – 1995. – P. 73–79.
14. *Ustimenko V.* Linguistic dynamical systems, graphs of large girth and cryptography // J. Math. Sci. – **140**, No 3. – P. 412–434.
15. *Romanczuk U., Ustimenko V.* On the key exchange with new cubical maps based on graphs // Annales UMCS Informatica AI XI. – 2011. – **4**. – P. 11–19.

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

Поступило в редакцию 07.06.2012

В. О. Устименко

Про екстремальну теорію графів і символьні перетворення

Мінімальну довжину цикла, що проходить крізь обрану вершину простого графу, назвемо цикловим показником вершини. Цикловий показник графу визначимо як найбільший цикловий показник його вершини. Регулярний граф називається графом з ірегулярним цикловим показником, якщо його цикловий показник відрізняється від обхвату. В роботі наводиться повний розв'язок оптимізаційної задачі обчислення максимального розміру $e = e(v)$ графів заданого порядку v з цикловим показником, що перевищує обраний параметр d, $d > 2$. Розглядається також задача знаходження найменшого порядку для k-регулярного графу з цикловим показником d. Наводиться алгебраїчна конструкція нескінченної сім'ї регулярних графів заданого степеня зі зростаючим ірегулярним цикловим показником асимптотично максимального розміру. Побудована нескінченна послідовність графів заданого степеня p^s, де p — довільне непарне просте, а s — довільне натуральне число, утворює сім'ю графів малого світу. Обговорюється криптографічне застосування цієї конструкції.

V. A. Ustimenko

On the extremal graph theory and symbolic computations

Let us refer to the minimal length of a cycle passing through the given vertex of a simple graph as the cycle indicator of this vertex. The cycle indicator of a graph will be defined as the maximal cycle indicator of its vertices. A regular graph will be called the graph with irregular cycle indicator if this indicator differs from the girth. The solution of the optimization problem of computation of the maximal size $e = e(v)$ of a graph of order v with the size greater than d, $d > 2$, is given. We consider also the algebraic construction of an infinite family of regular graphs of the given degree with growing irregular cycle indicator of the asymptotically largest size. The constructed sequence of graphs with the given degree p^s, where p is an arbitrary odd prime and s is any positive integer, forms the family of small-world graphs. We discuss the cryptographical applications of this construction.