пов голосования не приводит к усложнению обработки. Рассмотренный спектр подходов к корреляционному голосованию позволяет провести качественный анализ и сделать выводы по применению в практических задачах.

Научная новизна предложенного метода на основе голосования фрагментов состоит в обосновании моделей иерархической меры для сопоставления изображений, которая нацелена на повышение эффективности процедур распознавания в условиях неполной информации об анализируемых объектах.

Практическая значимость подхода заключается в повышенной устойчивости к локальным помехам по сравнению с классическими подходами при сохранении достаточной помехозащищенности к шуму, что подтверждается экспериментами на реальных полутоновых изображениях.

Несомненным достоинством подхода являются его универсальность в плане учета разнообразия возможных условий, возникающих при распознавании визуальных объектов.

Дальнейшие исследования будут направлены на теоретическое обоснование правил принятия решений по множеству отношений фрагментов.

### *ПЕРЕЧЕНЬ ССЫЛОК*

1. *Гороховатский В. А.* Распознавание изображений в условиях неполной информации / Гороховатский В. А. – Харьков : ХНУРЭ, 2003. – 112 с.
2. *Баклицкий В. К.* Методы фильтрации сигналов в корреляционно-экстремальных системах навигации / Баклицкий В. К., Бочкарев А. М., Мусьяков М. П. – Москва : Радио и связь, 1986. – 216 с.
3. *Гороховатский В. А.* Структурно-иерархические методы определения сходства изображений объектов // АСУ и приборы автоматики. – 2005. – Вып. 131. – С. 55–62.
4. *Шапиро Л.* Компьютерное зрение : пер. с англ. / Шапиро Л., Стокман Дж. – М. : Бином. 2006. – 752 с.
5. *Гороховатский В. А.* Применение процедур голосования в структурных методах распознавания визуальных объектов / Гороховатский В. А. // Вестник НТУ ХПИ. Системный анализ, управление и информационные технологии. – 2006. – № 39. – С. 132–140.
6. *Kim S.* Biologically motivated perceptual feature: generalized robust invariant feature / Kim S., Kweon I.-S. // Asian Conference of Computer Vision (ACCV-06), 2006. – P. 305–314.
7. *Путятин Е. П.* Распознавание изображений в пространстве инвариантных локальных признаков / Путятин Е. П., Гороховатский В. А., Кузьмин С. В. // Радиоэлектроника и информатика. – 2006. – № 1(32). – С. 69–73.
8. *Путятин Е. П.* Обработка изображений в робототехнике / Путятин Е. П., Аверин С. И. – М. : Машиностроение, 1990. – 320 с.

Надійшла 16.05.2008

*Наведено результати досліджень із застосування процедур голосування у кореляційних методах розпізнавання зображень. Вивчено способи формування систем фрагментів, формалізована постановка задачі розпізнавання, проаналізовано різноманітні варіанти голосування, шляхи вибору ознак фрагментів та встановлення відповідності між ними. Експериментальні результати підтверджують ефективність застосування підходу.*

*The results of application of voting procedures in correlation methods of image recognition are shown. The ways of systems of fragments construction are studied. The recognition problem is formalized. The variety of voting procedures, the ways of choosing fragment characteristics and the estab-lishment of the conformity between them are analyzed. The efficiency of the suggested approach is experimentally.*

*УДК 519.85*

И. В. Гребенник, А. В. Баранов

# ОЦЕНКИ МИНИМУМА ВЫПУКЛЫХ ФУНКЦИЙ НА КЛАССАХ КОМБИНАТОРНЫХ МНОЖЕСТВ ПЕРЕСТАНОВОК

*Исследуются задачи оптимизации выпуклых функций на комбинаторных множествах. Строятся оценки минимума выпуклых функций для классов комбинаторных множеств перестановок, при наличии или отсутствии линейных ограничений на переменные. Построение оценок включает в себя дополнительную процедуру оптимизации. Приводятся примеры, анализируются результаты вычислительных экспериментов.*

### *ВВЕДЕНИЕ*

При математическом моделировании классические комбинаторные множества часто с избытком описывают область допустимых решений комбинаторных оптимизационных задач [1]. В работе [2] введен новый класс комбинаторных множеств – композиционные образы комбинаторных множеств, которые позволяют более адекватно описывать области допустимых решений сложных задач комбинаторной оптимизации. Для решения задач оптимизации на композиционных образах комбинаторных множеств необходимо применять методы комбинаторной оптимизации, которые бы учитывали особенности введенного класса комбинаторных множеств.

Один из подходов к решению комбинаторных оптимизационных задач основан на декомпозиции множества допустимых решений с дальнейшей оценкой минимума функции цели на подмножествах [3, 4]. Условием применения такого подхода является наличие эффективных оценок минимума функций на множестве допустимых решений и его подмножествах. Исследование оценок минимума проведем для класса выпуклых функций.

Целью работы является построение эффективных оценок минимума выпуклых функций на классах комбинаторных множеств перестановок с учетом линейных ограничений на переменные.

## *ПОСТАНОВКА ЗАДАЧИ*

Рассматривается следующая задача оптимизации:

$$k(\alpha) \to \text{extr},$$
$$\alpha \in A \subseteq M, \qquad (1)$$

где $M$ – комбинаторное множество, $k: M \to R^1$.

В качестве $M$ могут выступать различные комбинаторные множества [5] в том числе и множества с более сложной структурой – композиционные образы комбинаторных множеств [2, 6]. В работе рассматриваются два представителя класса композиционных образов комбинаторных множеств: композиция перестановок и перестановки кортежей. Результаты исследования данных множеств представлены в работах [2, 6, 7]. Приведем основные результаты.

## *ПЕРЕСТАНОВКИ КОРТЕЖЕЙ И КОМПОЗИЦИЯ ПЕРЕСТАНОВОК*

Обозначим композиционный образ комбинаторных множеств $P_{nk}$, $T_1$, $T_2$, …, $T_n$, порожденный множествами $\{z_1^1, z_2^1, \ldots, z_m^1\}$, $\{z_1^2, z_2^2, \ldots, z_m^2\}$, …, $\{z_1^n, z_2^n, \ldots, z_m^n\}$. Здесь $T_i = \{(z_1^i, z_2^i, \ldots, z_m^i)\}$ – кортеж, составленный из элементов множества $\{z_1^i, z_2^i, \ldots, z_m^i\}$, $z_j^i \in R$, $i \in J_n = \{1, 2, \ldots, n\}$, $j \in J_m$. При этом среди $n$ множеств $T_i$ являются различными. Обозначим это множество через $PT_{nk}(T_1, T_2, \ldots, T_n)$ или $PT_{nk}^m$ и назовем множеством перестановок кортежей. Множество $PT_{nk}^m$ представляет собой множество перестановок кортежей $z^i = (z_1^i, z_2^i, \ldots, z_m^i)$, то есть упорядоченных наборов вида $w \in PT_{nk}^m$, $w = (z^{i_1}, z^{i_2}, \ldots, z^{i_n}) = (z_1^{i_1}, z_2^{i_1}, \ldots, z_m^{i_1}, z_1^{i_2}, z_2^{i_2}, \ldots, z_m^{i_2}, \ldots, z_1^{i_n}, z_2^{i_n}, \ldots, z_m^{i_n})$, где $i_s, j_s \in J_n$, $i_s \neq j_s$, $s \in J_n$. Элементы множества $PT_{nk}^m$ отличаются друг от друга только порядком следования кортежей $z^i$ в наборах.

Рассмотрим композиционный образ комбинаторных множеств $P_{nk}$, $P_{m_1k_1}$, $P_{m_2k_2}$, …, $P_{m_nk_n}$ порожденный множествами $\{a_1^1, a_2^1, \ldots, a_{m_1}^1\}$, $\{a_1^2, a_2^2, \ldots, a_{m_1}^2\}$, …, $\{a_1^n, a_2^n, \ldots, a_{m_n}^n\}$. Здесь $P_{nk}$ – множество перестановок из $n$ элементов, из которых являются различными, $a_i^j \in R^1$, $i \in J_{m_i}$, $j \in J_n$. Такое множество назовем композицией перестановок и обозначим $PW_N$. Множество $PW_N$ состоит из элементов вида $(e_{i_1}, e_{i_2}, \ldots, e_{i_n})$, где $(i_1, i_2, \ldots, i_n) \in L_n$, $e_i = (a_{s_1}^i, a_{s_2}^i, \ldots, a_{s_{m_i}}^i)$, $i \in J_n$. В наборе $(e_{i_1}, e_{i_2}, \ldots, e_{i_n})$ $k$ элементов являются различными, среди элементов $a_{s_1}^j, a_{s_2}^j, \ldots, a_{s_{m_j}}^j$ ровно $k_j$ различных. Таким образом, элементы множества $PW_N$ будут различаться порядком следования кортежей $e_i$ и элементов внутри кортежей.

Произведем погружение комбинаторного множества $M$ в евклидово пространство [8]. В результате погружения каждому элементу комбинаторного множества ставится во взаимно однозначное соответствие точка пространства $R^N$:

$$f: M \to R^N, \quad \forall \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_N) \in M,$$
$$x = f(\alpha) = (x_1, x_2, \ldots, x_N) \in E \subset R^N, \quad x_i = \alpha_i,$$
$$i \in J_N = \{1, 2, 3, \ldots, N\}.$$

Сформулируем следующую эквивалентную задачу оптимизации в евклидовом пространстве:

$$\Phi(x) \to \min,$$
$$x \in X \subseteq E_z \subset R^N, \qquad (2)$$

где $x = f(\alpha)$, $\varphi(x) = \kappa(\alpha)$ $\forall \alpha \in M$, $X = f(A)$, $E_z = f(M)$. В качестве множества $M$ могут выступать множество $P_{nk}$ перестановок из $n$ элементов, $k$ из которых различны, множество перестановок кортежей $PT_{nk}^m$ или композиция перестановок $PW_N$ и другие комбинаторные множества. Обозначим $E_{nk} = f(P_{nk})$, $ET_{nk}^m = f(PT_{nk}^m)$, $EW_N = f(PW_N)$.

Используя известные методы [9, 10], построим выпуклое (сильно выпуклое с параметром $\rho$) продолжение $\varphi(x)$ функции цели $\Phi(x)$ задачи (2) на выпуклое множество $V \supseteq \text{conv}E_z$, где $\text{conv}E_z$ – выпуклая оболочка множества $E_z$. В результате такого построения получим выпуклую или сильно выпуклую функцию $\varphi(x)$, которая в точках комбинаторного множества $E_z$ принимает те же значения, что и исходная функция $\Phi(x)$, т. е. $\varphi(x) = \Phi(x)$ для $\forall x \in E_z$. В ряде случаев множество допустимых решений $X \subseteq E_z$ можно описать с помощью системы линейных неравенств.

Тогда задача (2) может быть заменена следующей задачей оптимизации:

$$\varphi(x) \to \min,$$
$$Cx \le d,$$
$$x \in E_z, \qquad (3)$$

где $\varphi(x)$ – выпуклая (сильно выпуклая с параметром $\rho > 0$) на выпуклом множестве $V \supset \mathrm{conv}E_z$ функция, $C = [c_{ij}]_{m \times n}$, $c_{ij} \in R$, $d \in R^n$.

С целью разработки методов решения задачи (3) построим оценки минимума функции $\varphi(x)$ на множестве $P = \{x \mid x \in E_z \subset R^n, Cx \le d\}$, $x \in V$. Рассмотрим случаи, когда $E_z \in \{E_{nk}, ET^m_{nk}, EW_N\}$.

Воспользуемся оценками минимума выпуклых и сильно выпуклых функций на евклидовых комбинаторных множествах без дополнительных ограничений на переменные, полученными в работах [3, 14].

Пусть $\varphi(x)$ – выпуклое дифференцируемое продолжение функции $\Phi(x)$ на выпуклое множество $V \supset \mathrm{conv}E_z$. Тогда для любого $x \in V$ справедливо:

$$\min_{y \in P} \varphi(y) \ge \varphi(x) - (\nabla\varphi(x), x) + \min_{y \in P} (\nabla\varphi(x), y). \quad (4)$$

Для случая, когда $\varphi(x)$ – сильно выпуклое с параметром $\rho > 0$ продолжение на $V \supset \mathrm{conv}E_z$, справедлива следующая оценка:

$$\min_{y \in P} \varphi(y) \ge \varphi(y^*) + \rho \cdot \min_{y \in P} \|y - y^*\|^2, \qquad (5)$$

где $y^* = \arg\min_{y \in V} \varphi(y)$.

Если $\varphi(x)$ – сильно выпуклое дифференцируемое с параметром $\rho > 0$ продолжение, на выпуклое множество $V \supset \mathrm{conv}E_z$, тогда

$$\min_{y \in P} \varphi(y) \ge \varphi(x) - \frac{1}{4\rho}\|\nabla\varphi(x)\|^2 + \rho \min_{y \in P} \left\| y - x + \frac{1}{2\rho}\nabla\varphi(x) \right\|^2. \qquad (6)$$

Для вычисления численных значений оценок (4)–(6) необходимо решить задачи двух типов в их правых частях. Первая задача представляет собой задачу оптимизации линейной функции:

$$\sum_{j=1}^{N} \frac{\partial\varphi(x)}{\partial x_j} y_j \to \min, \quad y \in P. \qquad (7)$$

Решению задачи (7) посвящены работы [11–12]. Однако ни один из предложенных в них методов не является универсальным.

Вторая задача – это задача нахождения минимума нормы разности:

$$g(y) = \|y - d\|^2 = \sum_{i=1}^{N} (y_i - d_i)^2 \to \min_{y \in P}, \qquad (8)$$

где $d = (d_1, d_2, \ldots, d_N)$, $d \in R^n$.

Задачи (7)–(8) решаются по-разному в зависимости от наличия или отсутствия ограничений не переменные и в зависимости от типа комбинаторного множества $E_z$. Если в задаче (3) нет дополнительных ограничений на переменные ($P = E_z$), тогда в этом случае решение можно выписать в явном виде [13].

Приведем решение задачи (7), когда $E_z$ представляет собой множество $EW_N$. Пусть множество $PW_N$ порождено множествами $\{e^i_1, e^i_2, \ldots, e^i_m\}$, $i \in J_n$. Согласно [13], решением задачи (7) будет точка $y^* = (y^*_1, y^*_2, \ldots, y^*_N) \in EW_N$, где $y^*_{(j-1)m+r_t} = e^{i_j}_{s_t}$, $t \in J_m$, $j \in J_n$, $\{r_1, r_2, \ldots, r_m\}$ и $\{s_1, s_2, \ldots, s_m\}$ таковы, что $c_{(j-1)m+s_1} \ge c_{(j-1)m+s_2} \ge \ldots \ge c_{(j-1)m+s_m}$ и $e^{i_j}_{r_1} \le e^{i_j}_{r_2} \le \ldots \le e^{i_j}_{r_m}$, а последовательность $\{i_1, i_2, \ldots, i_m\}$ удовлетворяет условию $e_{i_1} \underset{c}{\prec} e_{i_2} \underset{c}{\prec} \ldots \underset{c}{\prec} e_{i_n}$, при $c = \nabla\varphi(x)$. Здесь $\underset{c}{\prec}$ – введенное отношение порядка:

$$e_{i_j} \underset{c}{\prec} e_{i_k} \Leftrightarrow (e^{i_j}_1, e^{i_j}_2, \ldots, e^{i_j}_m) \underset{c}{\prec} (e^{i_k}_1, e^{i_k}_2, \ldots, e^{i_k}_m) \Leftrightarrow$$
$$\Leftrightarrow \left( \left( \sum_{t=1}^{m} c_{(j-1)m+s_t} e^{i_j}_{p_t} + \sum_{t=1}^{m} c_{(k-1)m+r_t} e^{i_k}_{q_t} - \right. \right.$$
$$\left. \left. - \sum_{t=1}^{m} c_{(j-1)m+\alpha_t} e^{i_k}_{\gamma_t} - \sum_{t=1}^{m} c_{(k-1)m+\beta_t} e^{i_j}_{\delta_t} \right) \le 0 \right),$$

где $i \in J_n$, а последовательность индексов удовлетворяет условиям:

$$\{s_1, s_2, \ldots, s_m\} : c_{(j-1)m+s_1} \ge c_{(j-1)m+s_2} \ge \ldots \ge c_{(j-1)m+s_m},$$
$$\{p_1, p_2, \ldots, p_m\} : e^{i_j}_{p_1} \le e^{i_j}_{p_2} \le \ldots \le e^{i_j}_{p_m},$$
$$\{q_1, q_2, \ldots, q_m\} : e^{i_k}_{q_1} \le e^{i_k}_{q_2} \le \ldots \le e^{i_k}_{q_m},$$
$$\{r_1, r_2, \ldots, r_m\} : c_{(k-1)m+r_1} \ge c_{(k-1)m+r_2} \ge \ldots \ge c_{(k-1)m+r_m},$$
$$\{\alpha_1, \alpha_2, \ldots, \alpha_m\} : c_{(j-1)m+\alpha_1} \ge c_{(j-1)m+\alpha_2} \ge \ldots \ge c_{(j-1)m+\alpha_m},$$
$$\{\gamma_1, \gamma_2, \ldots, \gamma_m\} : e^{i_j}_{\gamma_1} \le e^{i_j}_{\gamma_2} \le \ldots \le e^{i_j}_{\gamma_m},$$
$$\{\delta_1, \delta_2, \ldots, \delta_m\} : e^{i_k}_{\delta_1} \le e^{i_k}_{\delta_2} \le \ldots \le e^{i_k}_{\delta_m},$$
$$\{\beta_1, \beta_2, \ldots, \beta_m\} : c_{(k-1)m+\beta_1} \ge c_{(k-1)m+\beta_2} \ge \ldots \ge c_{(k-1)m+\beta_m}.$$

Если область допустимых решений задачи (3) ограничена линейными ограничениями $P \subset E_z$, тогда для решения задач (7)–(8) можно использовать известные методы комбинаторной оптимизации, описан-

ные в [1]. Однако эти методы при больших размерностях задачи требуют больших вычислительных и временных ресурсов. В [14] предложен подход к решению поставленных задач на основе случайного поиска.

Отметим, что с одной стороны оценки (4)–(6) зависят от выбора точки $x \in V$, с другой стороны конструктивные методы построения сильно выпуклых продолжений позволяют построить сильно выпуклое продолжение для любого $\rho > 0$. Это дает возможность проводить оптимизацию значений правых частей соотношений (4)–(6) по этим параметрам. Введем следующие обозначения:

$$\overline{e}_1(x) = \varphi(x) - (\nabla\varphi(x), x) + \min_{y \in P}(\nabla\varphi(x), y), \qquad (9)$$

$$\overline{e}_2(\rho) = \varphi(y^*) + \rho \cdot \min_{y \in P}\|y - y^*\|^2, \qquad (10)$$

$$\overline{e}_3(x, \rho) = \varphi(x) - \frac{1}{4}\|\nabla\varphi(x)\|^2 + \rho \min_{y \in P}\left\|y - x + \frac{1}{2\rho}\nabla\varphi(x)\right\|^2. \qquad (11)$$

Эффективными оценками минимума будут являться такие оценки, которые максимально приближаются к решению задачи (3). Следовательно, необходимо стремиться к получению возможно больших по величине оценок (4)–(6). Исходя из этого, можно сформулировать следующие задачи оптимизации:

$$\overline{e}_1(x) \to \max, \quad x \in V, \qquad (12)$$

$$\overline{e}_2(\rho) \to \max, \quad \rho > \rho_0, \qquad (13)$$

$$\overline{e}_3(x, \rho) \to \max, \quad x \in V, \quad \rho > \rho_0. \qquad (14)$$

Аналитическое решение задач (12)–(14) затруднено из-за сложности выражений (9)–(11). Поэтому эти задачи могут быть решены численно с использованием методов недифференцируемой оптимизации.

Для иллюстрации предложенного подхода проведены серии вычислительных экспериментов. Рассмотрим в качестве целевой функции задачи (3) квадратичную функцию вида

$$\varphi(x) = (Ax, x) + (B, x) \to \min, \qquad (15)$$

где $A = [a_{ij}]_{m \times n}$ – положительно определенная симметричная матрица, $a_{ij} \in R$, $B \in R^n$, $x \in R^n$.

Сгенерируем случайным образом исходные данные задачи (3): матрицы $A$ и $B$, элементы, порождающие перестановки множества $E_z \in \{E_{nk}, ET^m_{nk}, EW_N\}$.

В первой серии экспериментов для задач небольшой размерности сравнивались значения оценок и точное решение задачи, полученное путем полного перебора.

Оценки (4)–(6) рассчитывались в случайно сгенерированной точке $x \in V$. После этого решались задачи оптимизации оценок (12)–(14) с помощью метода деформируемого многогранника. Для решения задач (7)–(8) при $P \subset E_z$ использовался метод на основе случайного поиска, описанный в [14]. Для случая $P = E_z$ решение задач (7)–(8) приведено в [13].

Для каждой тестовой задачи вычислялась характеристика $d_l$, характеризующая в долях единицы степень приближения оценки к точному решению задачи. Результаты экспериментов представлены в табл. 1 и 2. Здесь $e_l$ – значение оценок в тестовой точке, $e^*_l$ – значение оценок при оптимальных значениях параметра $\rho$ и точки $x \in V$, $t_l$ – время, затраченное на вычисление $e_l$, $t^*_l$ – время, затраченное на решение задач (12)–(14), $l = 1$ соответствует оценке (4), $l = 2$ – оценке (5), $l = 3$ – оценке (6).

Отметим, что в результате оптимизации, оценки $e_1$ и $e_3$ удалось приблизить к точному решению в среднем на 70–80 процентов (см. рис. 1 и рис. 2). Оценка $e_2$ оказалось неэффективной т. к. удалось ее усилить лишь незначительно. Отметим также, что с ростом размерности растет значение $t^*_l$. Для решения задачи размерностью 3 переменные требуется порядка 1 секунды. На решение задачи в 15 переменных уходит 35 секунд (для случая $P = E_z$) и более 300 секунд для случая $P \subset E_z$.

## *ВЫВОДЫ*

В результате проведения вычислительных экспериментов можно сделать следующие выводы:

1. Предложенные в работе оценки минимума выпуклых функций на комбинаторных множествах с дополнительной оптимизацией могут быть использованы при разработке методов комбинаторной оптимизации.

2. Разработанная схема оптимизации оценок позволяет получить эффективные оценки минимума выпуклых функций на различных классах комбинаторных множеств перестановок.

3. Значения оценок на классах множеств перестановок в значительной мере зависят от выбора точки $x \in V$. Изменяя параметр $\rho$, удалось достичь лишь незначительного улучшения оценок.

4. Для получения эффективных оценок необходимы значительные временные затраты, что ограничивает их применение при решении задач комбинаторной оптимизации.

*Таблица 1 – Результаты для случая* $P = E_z$

| Множество | N | Решение перебором | e1 | t1 | e1* | t1* | e2 | t2 | e2* | t2* | e3 | t3 | e3* | t3* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Перестановки | 3 | 48,743 | 27,751 | 0 | 43,438 | 0,907 | 11,613 | 0,031 | 13,36037 | 0,031 | 34,39268 | 0,016 | 44,07882 | 0,906 |
| Перестановки | 3 | 54,194 | 17,448 | 0 | 47,431 | 0,812 | 20,139 | 0 | 22,43923 | 0,062 | 33,00047 | 0 | 51,27682 | 0,89 |
| Перестановки | 3 | 276,953 | 37,002 | 0 | 271,39 | 0,89 | 52,661 | 0 | 55,16545 | 0,031 | 82,96092 | 0 | 270,9396 | 0,953 |
| Перестановки | 3 | 277,755 | 41,117 | 0,016 | 277,17 | 0,875 | 3,5 | 0 | 6,844044 | 0,032 | 44,44256 | 0,015 | 275,8179 | 0,89 |
| Итого: | | | 0,29323 | 0,004 | 0,936 | 0,871 | 0,203151 | 0,0078 | 0,227995 | 0,039 | 0,44352 | 0,0078 | 0,955449 | 0,9098 |
| Перестановки | 5 | 142,714 | 40,234 | 0 | 133,89 | 5,75 | 16,584 | 0,016 | 18,93727 | 0,125 | 54,53409 | 0 | 132,3802 | 5,797 |
| Перестановки | 5 | 221,73 | 57,017 | 0 | 207,07 | 5,641 | 70,434 | 0 | 71,08309 | 0,11 | 112,8817 | 0 | 215,864 | 5,562 |
| Перестановки | 5 | 185,348 | 23,455 | 0 | 169,35 | 5,516 | 98,764 | 0 | 98,8419 | 0,11 | 112,0199 | 0,016 | 181,1698 | 5,656 |
| Перестановки | 5 | 188,611 | 33,482 | 0,015 | 171,82 | 5,437 | 73,205 | 0 | 76,23711 | 0,188 | 99,98797 | 0 | 174,7204 | 5,297 |
| Итого: | | | 0,21078 | 0,00375 | 0,9242 | 5,586 | 0,338711 | 0,004 | 0,34769 | 0,1333 | 0,502454 | 0,004 | 0,951236 | 5,578 |
| Перестановки | 7 | 705,467 | 152,381 | 0 | 680 | 19,969 | 1,705 | 0 | 6,850315 | 0,312 | 154,7837 | 0,015 | 683,3854 | 18,891 |
| Перестановки | 7 | 811,241 | 153,956 | 0 | 780,72 | 18,515 | 110,486 | 0 | 113,8706 | 0,312 | 252,9516 | 0 | 803,8381 | 17,515 |
| Перестановки | 7 | 1399,353 | 215,869 | 0,016 | 1391,3 | 18,578 | 7,768 | 0 | 13,67716 | 0,36 | 224,0457 | 0 | 1393,625 | 19,843 |
| Перестановки | 7 | 3594,738 | 327,008 | 0 | 3491,2 | 19,125 | 16,124 | 0 | 24,60428 | 0,296 | 346,1968 | 0,015 | 3470,361 | 18,39 |
| Итого: | | | 0,16275 | 0,004 | 0,9729 | 19,04675 | 0,037162 | 0 | 0,041674 | 0,32 | 0,196907 | 0,0075 | 0,98022 | 18,66 |
| Перестановки | 9 | 1111,002 | 248,235 | 0 | 1102,4 | 44,687 | 2,694 | 0 | 16,33206 | 1,234 | 179,4312 | 0,015 | 1077,531 | 45,094 |
| Перестановки | 9 | 1020,491 | 152,317 | 0,016 | 1043,2 | 48,25 | 60,778 | 0,016 | 63,59343 | 0,641 | 210,6034 | 0,015 | 1010,635 | 43,453 |
| Перестановки | 9 | 1515,991 | 286,367 | 0 | 1435,7 | 48,687 | 247,78 | 0 | 249,5656 | 0,766 | 504,432 | 0 | 1487,154 | 66,75 |
| Итого: | | | 0,1872 | 0,005 | 0,9872 | 40,16769 | 0,075142 | 0,004 | 0,080546 | 0,7403 | 0,23354 | 0,0094 | 0,980398 | 43,489 |
| | | | | | | | | | | | | | | |
| d | | | **0,22235** | | **0,9529** | | **0,169435** | | **0,180738** | | **0,351476** | | **0,965921** | |
| | | | | | | | | | | | | | | |
| Перестановки кортежей | 6 | 1093,478 | 179,544 | 0 | 1069,6 | 0,688 | 114,655 | 0,016 | 120,0525 | 0,016 | 277,4021 | 0,016 | 1066,765 | 0,735 |
| Перестановки кортежей | 6 | 692,784 | 139,042 | 0 | 669,01 | 0,64 | 4,862 | 0 | 20,65569 | 0,015 | 143,5839 | 0 | 655,1095 | 0,625 |
| Перестановки кортежей | 6 | 574,452 | 140,22 | 0 | 540,41 | 0,625 | 0,397 | 0 | 6,873202 | 0,015 | 140,2894 | 0 | 534,8869 | 0,625 |
| Итого: | | | 0,203 | 0 | 0,9615 | 0,651 | 0,037521 | 0,0053 | 0,050523 | 0,0153 | 0,235053 | 0,0053 | 0,950772 | 0,6617 |
| Перестановки кортежей | 9 | 1349,911 | 407,293 | 0 | 1290,1 | 3,641 | 217,634 | 0 | 221,1199 | 0,063 | 571,7688 | 0 | 1323,31 | 3,359 |
| Перестановки кортежей | 9 | 2121,976 | 342,139 | 0 | 2030,9 | 3,468 | 264,186 | 0 | 268,2319 | 0,078 | 568,6559 | 0 | 2068,722 | 3,984 |
| Перестановки кортежей | 9 | 2971,78 | 329,088 | 0 | 2849,4 | 3,313 | 359,638 | 0 | 362,6842 | 0,062 | 653,7409 | 0 | 2911,814 | 3,734 |
| Итого: | | | 0,19123 | 0 | 0,9572 | 3,474 | 0,13558 | 0 | 0,137418 | 0,0677 | 0,303842 | 0 | 0,97834 | 3,6923 |
| Перестановки кортежей | 15 | 9096,509 | 1147,06 | 0 | 8871,5 | 25,937 | 374,014 | 0 | 429,1438 | 9,031 | 1488,741 | 0,016 | 9011,462 | 36,922 |
| Перестановки кортежей | 15 | 9521,55 | 881,625 | 0 | 9043 | 35,781 | 201,689 | 0 | 204,9972 | 0,281 | 1071,802 | 0 | 9251,163 | 32,578 |
| Перестановки кортежей | 15 | 9805,853 | 1252,97 | 0 | 9424,6 | 27,125 | 468,298 | 0,016 | 529,2077 | 5,687 | 1674,139 | 0 | 9535,955 | 27,296 |
| Итого: | | | 0,11549 | 0 | 0,962 | 29,61433 | 0,036685 | 0,0053 | 0,040892 | 4,9997 | 0,148985 | 0,0053 | 0,978243 | 32,265 |
| Перестановки кортежей | 21 | 34694,397 | 3156,85 | 0 | 33050 | 114,547 | 2570,552 | 0,016 | 2579,571 | 0,719 | 5554,523 | 0 | 34055,26 | 106,67 |
| Перестановки кортежей | 21 | 35023,626 | 2589,48 | 0 | 33422 | 116,61 | 1929,594 | 0,015 | 1936,703 | 0,703 | 4413,172 | 0,015 | 34110,74 | 87,781 |
| Перестановки кортежей | 21 | 34231,222 | 2180,47 | 0 | 32606 | 102,328 | 1969,38 | 0 | 1973,275 | 0,828 | 4067,414 | 0,015 | 33468,8 | 109,38 |
| Итого: | | | 0,07621 | 0 | 0,9522 | 111,1617 | 0,062239 | 0,0103 | 0,062431 | 0,75 | 0,134975 | 0,01 | 0,977747 | 101,28 |
| | | | | | | | | | | | | | | |
| d | | | **0,14648** | | **0,9582** | | **0,068006** | | **0,072816** | | **0,205714** | | **0,971275** | |
| | | | | | | | | | | | | | | |
| Композиция перестановок | 6 | 280,642 | 68,589 | 0 | 274,52 | 0,828 | 8,216 | 0 | 17,47516 | 0,422 | 75,78128 | 0 | 279,1113 | 0,859 |
| Композиция перестановок | 6 | 386,869 | 60,145 | 0 | 368,19 | 0,953 | 76,373 | 0 | 77,90764 | 0 | 128,3681 | 0 | 380,7694 | 0,937 |
| Композиция перестановок | 6 | 356,156 | 78,219 | 0,015 | 330,8 | 0,906 | 94,457 | 0 | 96,16537 | 0 | 157,017 | 0,016 | 340,2091 | 0,922 |
| Итого: | | | 0,2065 | 0,005 | 0,9529 | 0,895667 | 0,163967 | 0 | 0,177886 | 0,1407 | 0,347569 | 0,0053 | 0,978001 | 0,906 |
| Композиция перестановок | 9 | 965,988 | 198,465 | 0 | 883,56 | 5,813 | 32,445 | 0,015 | 36,92322 | 0,266 | 227,6009 | 0 | 965,7576 | 4,703 |
| Композиция перестановок | 9 | 1145,609 | 224,952 | 0 | 1084,1 | 5,203 | 202,466 | 0 | 220 | 1,5 | 398,7168 | 0,016 | 1098,249 | 4,938 |
| Композиция перестановок | 9 | 1640,767 | 246,538 | 0 | 1579,7 | 4,234 | 201,945 | 0 | 210,311 | 0 | 426,2045 | 0 | 1611,75 | 4,75 |
| Итого: | | | 0,18402 | 0 | 0,9412 | 5,083333 | 0,111133 | 0,005 | 0,11948 | 0,5887 | 0,281138 | 0,0053 | 0,980246 | 4,797 |
| Композиция перестановок | 15 | 5494,546 | 1071,4 | 0 | 5429,4 | 40,187 | 118,17 | 0,032 | 132,33 | 0,031 | 1172,018 | 0 | 5341,474 | 31,187 |
| Композиция перестановок | 15 | 4931,604 | 837,634 | 0 | 4912,1 | 38,5 | 198,31 | 0 | 204,0262 | 1,282 | 1011,951 | 0 | 4930,665 | 46,188 |
| Композиция перестановок | 15 | 10738,389 | 1027,86 | 0 | 10165 | 35,359 | 1200,569 | 0 | 1207,662 | 0,078 | 2144,659 | 0 | 10491,11 | 30,219 |
| Итого: | | | 0,15352 | 0 | 0,9769 | 38,01533 | 0,05784 | 0,0107 | 0,059306 | 0,4637 | 0,206074 | 0 | 0,982974 | 35,865 |
| | | | | | | | | | | | | | | |
| d | | | **0,18135** | | **0,957** | | **0,11098** | | **0,11889** | | **0,249924** | | **0,980407** | |

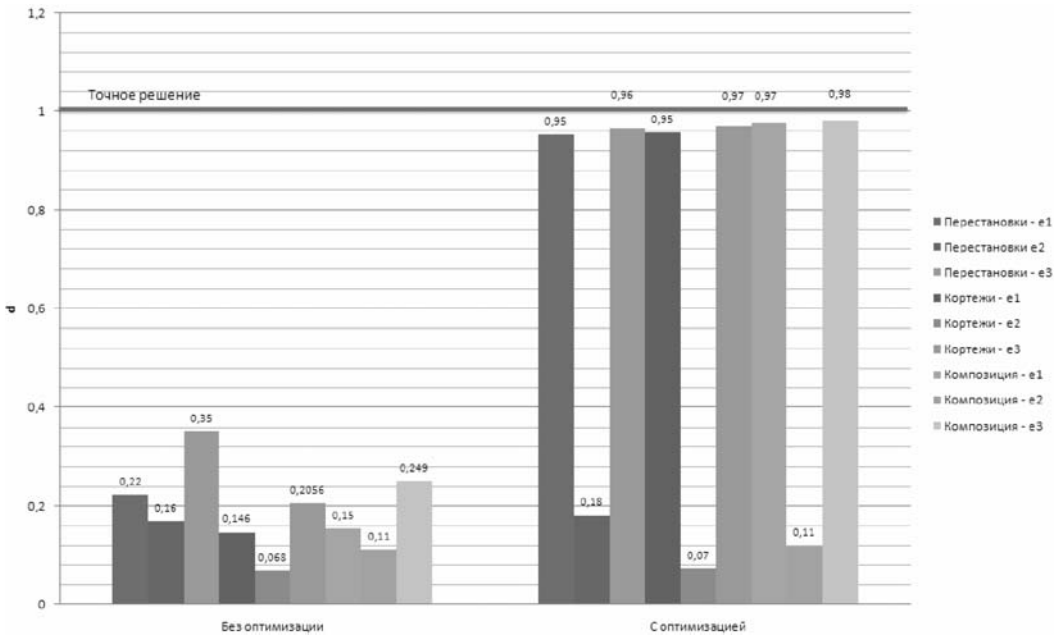


*Рисунок 1 – Повышение эффективности оценок для случая* $P = E_z$

*Таблица 2 – Результаты для случая* $P \subset E_2$

| Множество | N | Решение перебором | e1 | t1 | e1* | t1* | e2 | t2 | e2* | t2* | e3 | t3 | e3* | t3* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Перестановки | 3 | 130,5648 | 27,97 | 0,031 | 86,213 | 8,796 | 38,2226971 | 0 | 38,3742 | 0,234 | 49,65701 | 0,016 | 88,1947884 | 6,688 |
| Перестановки | 3 | 165,4793 | 47,623 | 0,032 | 159,53 | 17,22 | 80,8016279 | 0 | 80,94647 | 0,236 | 105,4669 | 0,014 | 169,789652 | 14,514 |
| Перестановки | 3 | 368,4078 | 58,459 | 0,016 | 283,56 | 3,312 | 194,693954 | 0 | 194,7628 | 0,236 | 225,8141 | 0 | 328,405453 | 2,282 |
| Итого: | | | 0,22023 | 0,02633 | 0,798 | 9,776 | 0,43650378 | 0 | 0,437245 | 0,2353 | 0,543537 | 0,01 | 0,86431756 | 7,828 |
| Перестановки | 5 | 150,7268 | 59,664 | 0,046 | 140,02 | 11,406 | 28,3087482 | 0,016 | 32,34756 | 1,234 | 75,53396 | 0,048 | 147,10201 | 21,5 |
| Перестановки | 5 | 258,7101 | 47,222 | 0 | 199,97 | 11,172 | 62,7102766 | 0 | 63,02255 | 0,28 | 99,9339 | 0,048 | 216,11929 | 31,454 |
| Перестановки | 5 | 236,2387 | 65,781 | 0,048 | 221,77 | 31,968 | 111,915318 | 0,016 | 114,4394 | 2,954 | 150,0744 | 0 | 235,422914 | 0,718 |
| Итого: | | | 0,28561 | 0,03133 | 0,8802 | 18,182 | 0,3013164 | 0,0107 | 0,314212 | 1,4893 | 0,507558 | 0,032 | 0,93595683 | 17,891 |
| Перестановки | 7 | 489,0209 | 112,893 | 0,094 | 493,83 | 145,952 | 51,3969791 | 0,032 | 54,37296 | 11,39 | 151,7258 | 0,094 | 501,506713 | 269,86 |
| Перестановки | 7 | 653,7975 | 175,549 | 0,093 | 639,94 | 112,844 | 36,6838532 | 0 | 37,27781 | 0,312 | 82,12835 | 0 | 548,929535 | 299,27 |
| Перестановки | 7 | 406,6976 | 156,599 | 0,109 | 388,27 | 46,687 | 57,9348175 | 0 | 69,90977 | 0,969 | 197,5128 | 0,078 | 410,825349 | 42,844 |
| Итого: | | | 0,2948 | 0,09867 | 0,9811 | 101,8277 | 0,10122084 | 0,0107 | 0,113367 | 4,2237 | 0,307177 | 0,0573 | 0,95842782 | 203,99 |
| | | | | | | | | | | | | | | |
| d | | | 0,26688 | | 0,8865 | | 0,27968034 | | 0,288275 | | 0,452758 | | 0,9195674 | |
| | | | | | | | | | | | | | | |
| Перестановки кортежей | 6 | 283,7951 | 99,779 | 0 | 269,98 | 4,812 | 12,0454933 | 0 | 15,92531 | 0,234 | 101,5113 | 0 | 281,197689 | 2,11 |
| Перестановки кортежей | 6 | 573,4659 | 102,098 | 0 | 571,27 | 0,813 | 18,2950123 | 0 | 21,0292 | 0,296 | 112,8657 | 0,015 | 573,304479 | 0,562 |
| Перестановки кортежей | 6 | 357,3262 | 94,318 | 0 | 326,14 | 0,938 | 43,1384911 | 0 | 44,10416 | 0,344 | 122,6423 | 0 | 357,177034 | 3,797 |
| Итого: | | | 0,26453 | 0 | 0,9534 | 2,187667 | 0,06502422 | 0 | 0,072071 | 0,2913 | 0,299243 | 0,005 | 0,99671622 | 2,1563 |
| Перестановки кортежей | 9 | 1226,7556 | 266,347 | 0 | 1199,7 | 63,906 | 20,9758875 | 0 | 28,42412 | 0,453 | 271,6677 | 0 | 1201,43827 | 60,734 |
| Перестановки кортежей | 9 | 1728,7176 | 419,965 | 0 | 1673,1 | 5,25 | 201,945 | 0 | 210,311 | 0,266 | 677,9389 | 0 | 1691,79771 | 6,141 |
| Итого: | | | 0,23002 | 0 | 0,9729 | 34,578 | 0,06695824 | 0 | 0,072414 | 0,3595 | 0,306808 | 0 | 0,97900278 | 33,438 |
| | | | | | | | | | | | | | | |
| d | | | 0,25073 | | 0,9612 | | 0,06579783 | | 0,072208 | | 0,302269 | | 0,98963084 | |
| | | | | | | | | | | | | | | |
| Композиция перестановок | 6 | 318,995 | 96,994 | 0,032 | 288,86 | 13,187 | 28,3905656 | 0 | 35,22979 | 0,469 | 116,514 | 0,031 | 297,436 | 11,57 |
| Композиция перестановок | 6 | 333,6153 | 132,812 | 0 | 336,77 | 45,734 | 20,2575928 | 0 | 23,77155 | 0,234 | 140,0707 | 0,016 | 342,350793 | 69,125 |
| Итого: | | | 0,35108 | 0,016 | 0,9575 | 29,4605 | 0,07486072 | 0 | 0,090847 | 0,3515 | 0,392555 | 0,0235 | 0,9793001 | 40,348 |
| Композиция перестановок | 9 | 1581,074 | 298,656 | 0,265 | 1471,2 | 596,515 | 270,284825 | 0,032 | 277,1776 | 23,86 | 521,6244 | 0,313 | 1542,05897 | 591,09 |
| Итого: | | | 0,18889 | 0,265 | 0,9305 | 596,515 | 0,17095014 | 0,032 | 0,17531 | 23,86 | 0,329918 | 0,313 | 0,97532372 | 591,09 |
| | | | | | | | | | | | | | | |
| d | | | 0,29702 | | 0,9485 | | 0,10689053 | | 0,119001 | | 0,371676 | | 0,97797464 | |

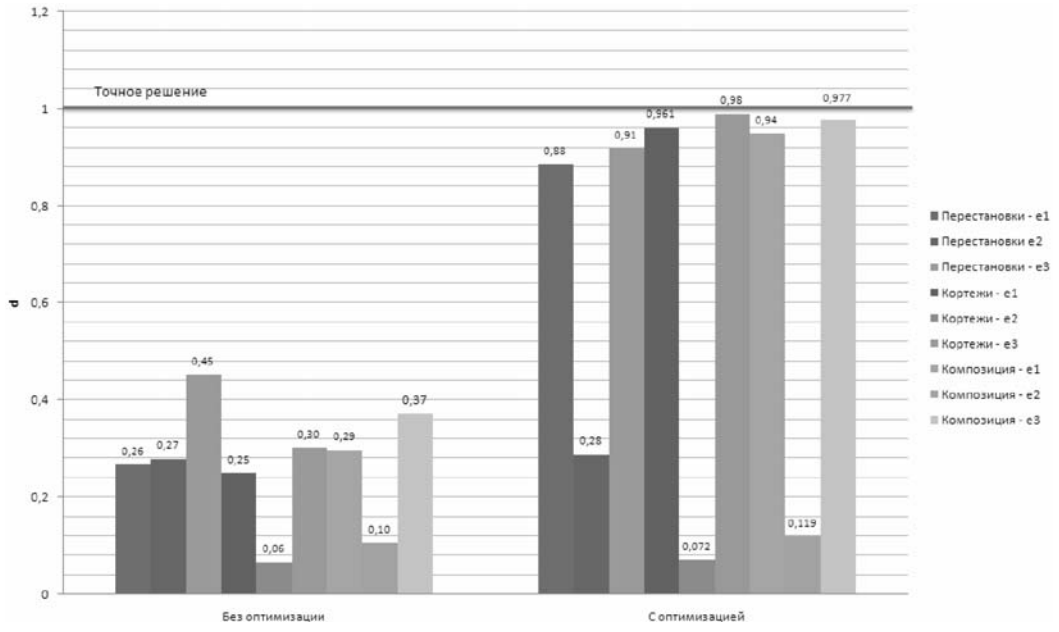


*Рисунок 2 – Повышение эффективности оценок для случая* $P \subset E_2$

## *ПЕРЕЧЕНЬ ССЫЛОК*


1. *Сергиенко И. В.* Математические модели и методы решения задач дискретной оптимизации / Сергиенко И. В. – К. : Наук. думка, 1988. – 472 с.
2. *Стоян Ю. Г.* Композиционные образы комбинаторных множеств и некоторые их свойства / Стоян Ю. Г., Гребенник И. В. // Пробл. машиностроения. – 2005. – Т. 8, № 3. – С. 56–62.
3. *Стоян Ю. Г.* Теорія і методи евклідової комбінаторної оптимізації / Стоян Ю. Г., Ємець О. О. – К. : ІСДО, 1993. – 188 с.
4. *Яковлев С. В.* О некоторых классах задач оптимизации на множествах размещений и их свойствах / Яковлев С. В., Гребенник И. В. // Изв. вузов. Математика. – 1991. – № 11. – С. 74–86.
5. *Айгнер М.* Комбинаторная теория / Айгнер М. – М. : Мир, 1982. – 558 с.
6. *Гребенник И. В.* Классы композиционных образов комбинаторных множеств в математических моделях задач геометрического проектирования / Гребенник И. В. // Радиоэлектроника и информатика. – 2005. – № 3. – С. 69–73.
7. *Гребенник И. В.* Оптимизация линейных функций на множестве композиций перестановок / Гребенник И. В., Баранов А. В. // Компьютерное моделирование и интеллектуальные системы : сборник научных трудов. – Запорожье : ЗНТУ, 2007. – С. 116–121.

8. *Стоян Ю. Г.* Математические модели и оптимизационные методы геометрического проектирования / Стоян Ю. Г., Яковлев С. В. – К. : Наук. думка, 1986. – 268 с.
9. *Яковлев С. В.* Теория выпуклых продолжений функции на вершинах выпуклых многогранников... / Яковлев С. В. // ЖВМ и МФ. – 1994. – Т. 34, № 7. – С. 1112–1119.
10. *Стоян Ю. Г.* Построение выпуклых и вогнутых функций на перестановочном многограннике / Стоян Ю. Г., Яковлев С. В. // ДАН УССР, Сер А. – 1988. – № 5. – С. 68–70.
11. *Яковлев С. В.* О минимизации линейной функции на вершинах перестановочного многогранника с учетом линейных ограничений / Яковлев С. В., Валуйская О. А. // Доп. НАНУ. – 1999. – № 11. – С. 103–107.
12. *Гребенник И. В.* Решение некоторых задач условной оптимизации линейных функций на перестановочном многограннике / Гребенник И. В. // Радиоэлектроника и информатика. – 1999. – № 1. – С. 55–59.
13. *Гребенник И. В.* Экстремальные свойства функций на классах композиционных образов комбинаторных множеств / Гребенник И. В., Баранов А. В. // Бионика интеллекта. – 2007. – № 1(66). – С. 99–102.
14. *Гребенник И. В.* Оптимизация линейных функций с линейными ограничениями на комбинаторных множествах на основе случайного поиска / Гребенник И. В., Баранов А. В. // Искусственный интеллект. – 2007. – № 1. – С. 132–137.

Надійшла 16.09.2008

*Досліджуються задачі оптимізації опуклих функцій на комбінаторних множинах. Будуються оцінки мінімумів опуклих функцій для класів комбінаторних множин перестановок, з урахуванням та без урахування лінійних обмежень на змінні. Побудова оцінок включає в себе додаткову процедуру оптимізації. Наводяться приклади, аналізуються результати обчислювальних експериментів.*

*The paper is devoted to the problem of convex functions optimization on combinatorial sets. Estimates of convex function minimum are constructed for different classes of combinatorial sets of permutations, with or without linear constraints on the variables. Estimates construction includes an addi-tional procedure of optimization. Examples are given; results of numerical experiments are analyzed.*

*УДК 681.3.06*

В. И. Долгов, А. В. Неласая

# МЕТОД ВЫЧИСЛЕНИЯ МАТРИЦЫ ХАССЕ – ВИТТА ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ СПЕЦИАЛЬНОГО ВИДА

*В статье предложен метод вычисления элементов матрицы Хассе – Витта гиперэллиптических кривых специального вида, основанный на использовании формулы бинома Ньютона.*

## *ВВЕДЕНИЕ*

Двухключевая криптография основана на трудности решения определенных математических задач. На первых порах развития этого направления такими задачами рассматривались разложения большого числа на простые множители и дискретное логарифмирование в простом поле Галуа. Современные стандарты цифровой подписи и направленного шифрования основаны на использовании операций в группах точек эллиптических кривых. Они обеспечивают меньшие длины параметров и, соответственно, более высокое быстродействие при сохранении заданного уровня стойкости. В частности, ныне действующий в Украине стандарт электронной цифровой подписи ДСТУ 4145-2002 основан на преобразованиях в группе точек эллиптических кривых, определенных над расширенными конечными полями $GF(2^m)$.

Естественным теоретическим и практическим обобщением эллиптических кривых являются гиперэллиптические кривые. Источником абелевой группы в этом случае выступает группа классов дивизоров (якобиан) гиперэллиптической кривой. Теория дивизоров гиперэллиптических кривых сегодня играет важную роль и при конструировании систем, основанных на спариваниях Вейля и Тейта, а также при решении задач дискретного логарифмирования на эллиптических кривых (метод спуска Вейля).

Основное преимущество при использовании гиперэллиптических кривых состоит в том, что размер основного поля, над которым определена кривая, уменьшается пропорционально роду кривой без потери стойкости, хотя сама формула группового сложения выглядит более громоздко.

Среди важных направлений совершенствования современных технологий применения гиперэллиптических кривых в криптографии можно выделить задачи, связанные с определением порядков якобианов кривых, которые и сегодня считаются вычислительно сложными [1, 2].

В этой работе предлагается метод вычисления элементов матрицы Хассе – Витта гиперэллиптической кривой, с использованием которой можно решить задачу определения порядка якобиана гиперэллиптической кривой [1, 2]. Этот метод требует для реализации существенно меньших вычислительных затрат по сравнению с известными. Он основан на использовании формулы бинома Ньютона и применим для кривых специального вида.