УДК 621.391

ИССЛЕДОВАНИЕ АЛГЕБРОГЕОМЕТРИЧЕСКИХ КОДОВ НА ПРОСТРАНСТВЕННЫХ КРИВЫХ АРТИН-ШРАЕРА ДЛЯ ПОВЫШЕНИЯ ПОМЕХОУСТОЙЧИВОСТИ ПЕРЕДАЧИ ДИСКРЕТНЫХ СООБЩЕНИЙ

Н.Н. Ляпа, В.И. Грабчак, И.В. Пасько
Военный институт РВиА Сумского государственного университета

Исследуется помехоустойчивость передачи дискретных сообщений с использованием алгеброгеометрических кодов на пространственных кривых Артин-Шраера.

ВВЕДЕНИЕ

Одним из перспективных направлений в развитии теории помехоустойчивого кодирования являются алгеброгеометрические коды. Недвоичные алгебраические блоковые коды, построенные по алгебраическим кривым (алгеброгеометрические коды), обладают хорошими асимптотическими свойствами, их применение позволяет исправлять сложные комбинации коррелированных ошибок, так называемые пакеты (пачки, группы) ошибок. Доказано, что при большой длине эти коды лежат выше границы Варшамова-Гилберта [1]. Использование этих кодов позволяет значительно снизить вероятность ошибочного приема дискретных сообщений и получить значительный энергетический выигрыш от кодирования [2, 3].

В то же время на сегодняшний день проведены исследования алгеброгеометрических кодов для плоских алгебраических кривых, заданных в проективном пространстве P^2 неприводимым однородным уравнением от трех переменных [4]. Перспективным направлением дальнейших исследований является исследование помехоустойчивости передачи дискретных сообщений с использованием алгеброгеометрических кодов на пространственных кривых, в частности на кривых Артин-Шраера, задаваемых в проективном пространстве P^3 совместными решениями совокупности двух однородных уравнений от четырех переменных [5].

Целью статьи является исследование алгеброгеометрических кодов на пространственных кривых Артин-Шраера для повышения помехоустойчивости передачи дискретных сообщений.

ОБОСНОВАНИЕ ВЫБОРА ПРОСТРАНСТВЕННЫХ КРИВЫХ АРТИН-ШРАЕРА ДЛЯ ПОВЫШЕНИЯ ПОМЕХОУСТОЙЧИВОСТИ ПЕРЕДАЧИ ДИСКРЕТНЫХ СООБЩЕНИЙ

Основная проблема теории избыточного кодирования, впервые сформулированная в работе К. Шеннона [6], состоит в поиске регулярных алгоритмов построения кодов с большой относительной скоростью R и с большим минимальным кодовым расстоянием d. Построение эффективных помехоустойчивых кодов в общетеоретическом плане сопряжено с построением длинных (с большим n) блоковых кодов, сохраняющих высокие конструктивные кодовые соотношения (n, k, d).

Анализ кодовых соотношений алгеброгеометрических кодов [4] показывает, что для кодов, заданных через порождающую матрицу, (n, k, d) параметры связаны соотношением

$$(n \le N,\ \ k \ge \alpha - g + 1,\ \ \ d \ge n - \alpha),$$

а для кодов, заданных через проверочную матрицу (дуальный код), –

$$(n \le N,\ \ k \ge n - \alpha + g - 1, \qquad d \ge \alpha - 2g + 2)\,.$$

Таким образом, задачу построения эффективных алгеброгеометрических кодов можно сформулировать следующим образом: найти регулярные методы построения линейных систем, возникающих на алгебраических кривых с большим числом точек N, по отношению к роду кривой g.

Обозначим через w – размерность пространства P^w, над которым определена кривая X, через $N(X_w)$ и $g(X_w)$ – соответствующее количество точек и род кривой X. Тогда общим критерием выбора алгебраических кривых для построения эффективных алгеброгеометрических кодов является выражение

$$\lim_{w\to\infty} \frac{N(X_w)}{g(X_w)} > 0\,.$$

На сегодняшний день по приведенному критерию исследовано множество плоских алгебраических кривых (кривых в P^2) [7]. Для пространственных кривых известна обобщенная конструкция Артин-Шраера (tower Artin-Schraier) над конечным полем $GF(p^2)$, которая задается следующим выражением

$$x_i^{p-1}x_{i+1}^p + x_{i+1} - x_i^p = 0\,,\ \ i = 0,\ 1,\ \ldots,\ w-2\,.$$

Для этой пространственной кривой известна оценка количества точек:

$$N(X_w) \ge (p^2-1)p^{w-1}\,,$$

и значение рода кривой

$$g(X_w) = \begin{cases} p^w + p^{w-1} - p^{\frac{w+1}{2}} - 2p^{\frac{w-1}{2}} + 1, & \text{если } w - \text{нечетное;} \\ p^w + p^{w-1} - \frac{1}{2}p^{\frac{w+2}{2}} - \frac{3}{2}p^{\frac{w}{2}} - p^{\frac{w-2}{2}} + 1, & \text{если } w - \text{четное.} \end{cases}$$

В работе [8] показано, что данная конструкция кривой достигает теоретической границы Дринфельда-Влэдуца

$$\lim_{g\to\infty} \frac{N_q(g)}{g} \le \sqrt{q} - 1\,,$$

которая устанавливает предельное значение отношения числа рациональных точек кривой над конечным полем $GF(q)$ рода g.

Таким образом, обобщенная конструкция Артин-Шраера может рассматриваться как реальный источник кривых для построения эффективных помехоустойчивых кодов.

ОЦЕНКА КОДОВЫХ СООТНОШЕНИЙ АЛГЕБРОГЕОМЕТРИЧЕСКИХ КОДОВ НА ПРОСТРАНСТВЕННЫХ КРИВЫХ АРТИН-ШРАЕРА И СРАВНЕНИЕ С ПАРАМЕТРАМИ НЕДВОИЧНЫХ КОДОВ БЧХ

Рассмотрим конструкцию Артин-Шраера для случая $w = 3$ (случай пространственных кривых в P^3). Получим пространственную кривую, заданную совокупностью решений двух однородных алгебраических уравнений от 4 переменных над $GF(p^2)$:

$$\begin{cases} f_1(x_0,x_1,x_2,x_3) = x_0^{p-1}x_1^p + x_1x_2^{2p-2} - x_0^p x_2^{p-1} = 0 \\ f_2(x_0,x_1,x_2,x_3) = x_1^{p-1}x_2^p + x_2x_3^{2p-2} - x_1^p x_3^{p-1} = 0 \end{cases}.$$

Род кривой и количество точек над $GF(p^2)$ удовлетворяют выражениям

$$g = p^3 - 2p + 1,$$
$$N \geq p^4 - p^2.$$

Отношение количества точек к роду кривой запишем в виде выражения

$$\frac{N}{g} \geq \frac{p^4 - p^2}{p^3 - 2p + 1},$$

что, несомненно, согласуется с вводами по достижении теоретической границы Дринфельда-Влэдуца.

Для практического использования алгеброгеометрических кодов на пространственных кривых рассмотрим конструкцию Артин-Шраера, построенную в P^2 над $GF(p^2)$, $p = 2^u$. Получим следующие уравнения кривых и соответствующие оценки количества точек и рода кривой.

Для случая $u = 1$: $p = 2$:

$$\begin{cases} f_1(x_0,x_1,x_2,x_3) = x_0x_1^2 + x_1x_2^2 - x_0^2x_2 = 0; \\ f_2(x_0,x_1,x_2,x_3) = x_1x_2^2 + x_2x_3^2 - x_1^2x_3 = 0; \end{cases}$$
$$g = 5, \quad N \geq 12 \quad \text{над } GF(4);$$

для случая $u = 2$: $p = 4$:

$$\begin{cases} f_1(x_0,x_1,x_2,x_3) = x_0^3x_1^4 + x_1x_2^6 - x_0^4x_2^3 = 0; \\ f_2(x_0,x_1,x_2,x_3) = x_1^3x_2^4 + x_2x_3^6 - x_1^4x_3^3 = 0; \end{cases}$$
$$g = 57, \quad N \geq 240 \quad \text{над } GF(16);$$

для случая $u = 3$: $p = 8$:

$$\begin{cases} f_1(x_0,x_1,x_2,x_3) = x_0^7x_1^8 + x_1x_2^{14} - x_0^8x_2^7 = 0; \\ f_2(x_0,x_1,x_2,x_3) = x_1^7x_2^8 + x_2x_3^{14} - x_1^8x_3^7 = 0); \end{cases}$$
$$g = 497, \quad N \geq 4032 \quad \text{над } GF(64);$$

для случая $u = 4$: $p = 16$:

$$\begin{cases} f_1(x_0,x_1,x_2,x_3) = x_0^{15}x_1^{16} + x_1x_2^{30} - x_0^{16}x_2^{15} = 0; \\ f_2(x_0,x_1,x_2,x_3) = x_1^{15}x_2^{16} + x_2x_3^{30} - x_1^{16}x_3^{15} = 0; \end{cases}$$
$$g = 4065, \quad N \geq 65280 \quad \text{над } GF(256);$$

для случая $u = 5$: $p = 32$:

$$\begin{cases} f_1(x_0,x_1,x_2,x_3) = x_0^{31}x_1^{32} + x_1x_2^{62} - x_0^{32}x_2^{31} = 0; \\ f_2(x_0,x_1,x_2,x_3) = x_1^{31}x_2^{32} + x_2x_3^{62} - x_1^{32}x_3^{31} = 0; \end{cases}$$
$$g = 32705, \quad N \geq 1047552 \quad \text{над } GF(1024).$$

Кодовые соотношения алгеброгеометрических кодов на пространственных кривых Артин-Шраера над $GF(4)$ удовлетворяют выражению

$$\begin{cases} n = 12 \\ k + d \geq 10. \end{cases}$$

На рис. 1 приведены соответствующие зависимости относительной скорости кодирования $R = k/n$ от относительного минимального кодового расстояния $\delta = d/n$ для алгеброгеометрических кодов на пространственных кривых Артин-Шраера над $GF(4)$ длины n = 12 (1), а так же граница недвоичных БЧХ кодов для $n = 12$ (2).

Для сравнения на рис. 1 также приведены верхняя кодовая граница Синлгтона (3) и нижняя кодовая граница Варшамова-Гилберта (4).

Из рисунка видно, что для R < 0,5 оценка кодовых соотношений алгеброгеометрических кодов на пространственных кривых Артин-Шраера дает лучший по сравнению с недвоичными БЧХ кодами результат. В то же время для этого алфавита символов алгеброгеометрические коды лежат ниже нижней теоретической границы Варшамова-Гилберта.

На рис. 2 приведены аналогичные зависимости для кодов над $GF(16)$ длины $n = 240$ (1) и соответствующая граница недвоичных БЧХ-кодов (2).

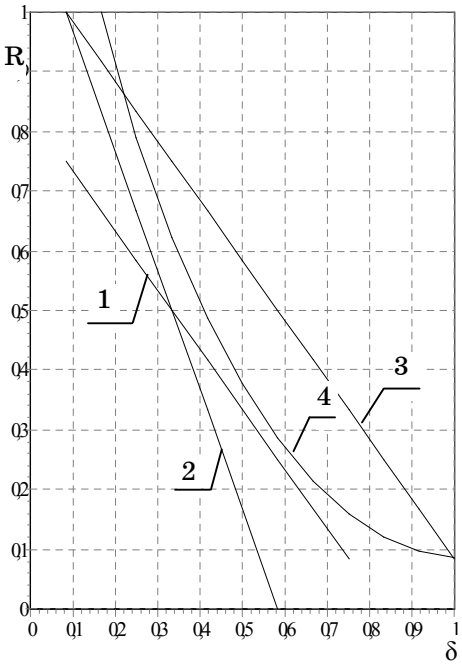

Рисунок 1 – Оценка кодовых соотношений алгеброгеометрических кодов на пространственных кривых Артин-Шраера над $GF(4)$

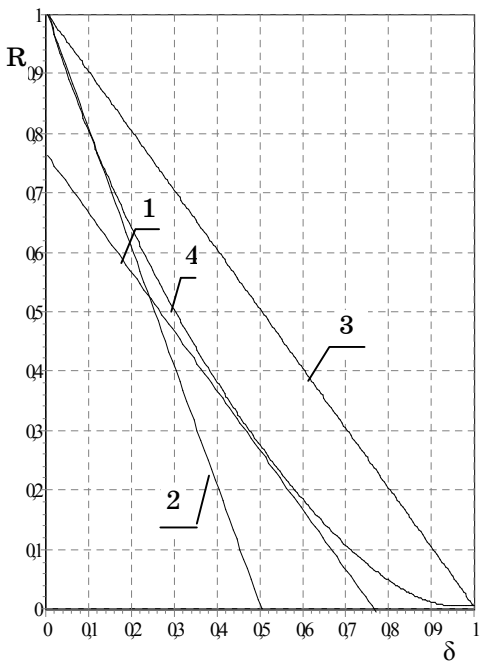

Рисунок 2 – Оценка кодовых соотношений алгеброгеометрических кодов на пространственных кривых Артин-Шраера над $GF(16)$

Кодовые соотношения алгеброгеометрических кодов на пространственных кривых Артин-Шраера над $GF(16)$ удовлетворяют выражению

$$\begin{cases} n = 240 \\ k + d \geq 184 \end{cases}.$$

Анализ рис. 2 позволяет сделать вывод об улучшении с ростом длины кода и мощности алфавита символов кодовых соотношений алгеброгеометрических кодов. Уже при $R < 0{,}53$ оценка кодовых соотношений алгеброгеометрических кодов на пространственных кривых Артин-Шраера дает лучший по сравнению с недвоичными БЧХ кодами результат. В то же время и для этого алфавита символов алгеброгеометрические коды лежат ниже нижней теоретической границы Варшамова-Гилберта.

Кодовые соотношения алгеброгеометрических кодов на пространственных кривых Артин-Шраера над $GF(64)$ удовлетворяют выражению

$$\begin{cases} n = 4032 \\ k + d \geq 3536. \end{cases}$$

На рис. 3 приведены соответствующие зависимости относительной скорости кодирования $R = k/n$ от относительного минимального кодового расстояния $\delta = d/n$ для алгеброгеометрических кодов над $GF(64)$ длины $n = 4032$ (1), а также граница недвоичных БЧХ-кодов для $n = 4032$ (2).

Как видно из рис. 3, алгеброгеометрические коды на пространственных кривых Артин-Шраера над $GF(64)$ с $0{,}1 < R < 0{,}65$ лежат выше нижней кодовой границы Варшамова-Гилберта и уже при $R < 0{,}75$ дают лучший по сравнению с БЧХ-кодами результат. Это свидетельствует о значительном преимуществе данного класса помехоустойчивых кодов по сравнению с лучшими известными результатами (недвоичными БЧХ-кодами).

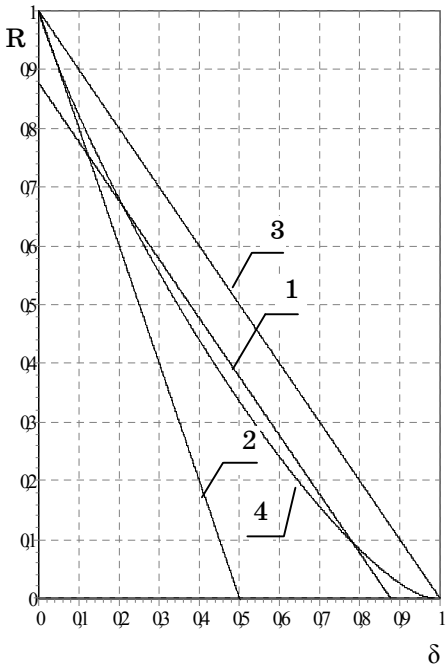

Рисунок 3 – Оценка кодовых соотношений алгеброгеометрических кодов на пространственных кривых Артин-Шраера над $GF(64)$

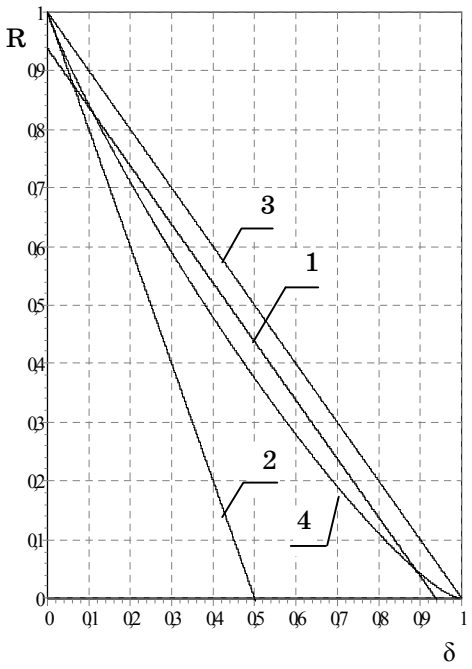

Рисунок 4–- Оценка кодовых соотношений алгеброгеометрических кодов на пространственных кривых Артин-Шраера над $GF(256)$

На рис. 4 приведены зависимости относительной скорости кодирования от относительного минимального кодового расстояния для алгеброгеометрических кодов над $GF(256)$ (1) и соответствующая граница недвоичных БЧХ-кодов (2).

Кодовые соотношения алгеброгеометрических кодов на пространственных кривых Артин-Шраера над $GF(256)$ удовлетворяют выражению

$$\begin{cases} n = 65280 \\ k + d \geq 61216. \end{cases}$$

Как видно из приведенных зависимостей, алгеброгеометрические коды с $0{,}04 < R < 0{,}83$ лежат выше нижней кодовой границы Варшамова-Гилберта и уже при $R < 0{,}88$ дают лучший по сравнению с БЧХ-кодами результат.

Кодовые соотношения алгеброгеометрических кодов на пространственных кривых Артин-Шраера над $GF(1024)$ удовлетворяют выражению

$$\begin{cases} n = 1047552 \\ k + d \geq 1014848. \end{cases}$$

На рис. 5 приведены зависимости $R = k/n$ от $\delta = d/n$ для алгеброгеометрических кодов над $GF(1024)$ (1) и соответствующая граница недвоичных БЧХ-кодов (2).

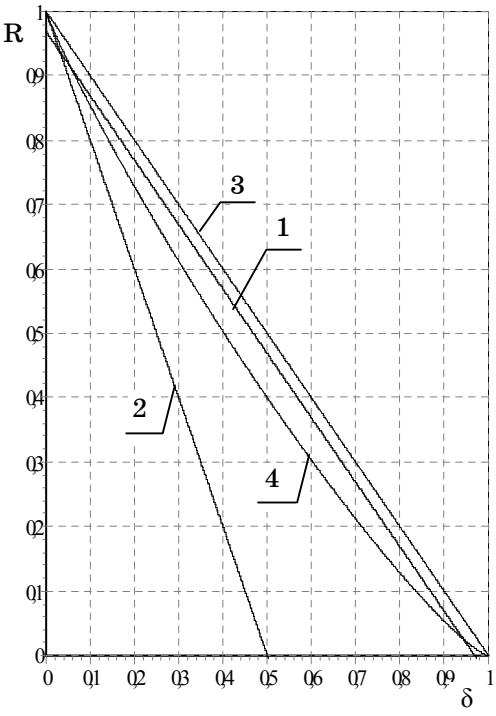

Рисунок 5 - Оценка кодовых соотношений алгеброгеометрических кодов на пространственных кривых Артин-Шраера над $GF(256)$

Анализ зависимостей, приведенных на рис. 5, показывает, что практически для всего диапазона относительной скорости кодирования алгеброгеометрические коды на пространственных кривых Артин-Шраера над $GF(1024)$ лежат выше нижней теоретической границы Варшамова-Гилберта и дают лучший по сравнению с недвоичными БЧХ-кодами результат.

Таким образом, как показывают проведенные исследования, алгебро-геометрические коды на пространственных кривых Артин-Шраера имеют кодовые соотношения, которые при увеличении длины кода и мощности алфавита символов стремятся к верхним теоретическим границам (границе Синлгтона).

В таблице 1 приведены экспериментальные оценки кодовых соотношений алгеброгеометрических кодов на пространственных кривых Артин-Шраера над $GF(4)$ и над $GF(16)$.

В таблице приведены оценки информационной длины слова k и кодового расстояния d, а также соответствующие параметры дуального кода ($k_\perp$ и $d_\perp$). Соответствующие

кодовые конструкции строились посредством отображения множества рациональных точек кривой с использованием набора генераторных функций – множества одночленов от четырех переменных степени $\deg F$. Соответствующая генераторная матрица использовалась в качестве порождающей (оценки k и d) и проверочной (оценки $k_\perp$ и $d_\perp$) матриц кода. Тестирование по кодовому расстоянию d и $d_\perp$ производилось путем перебора всех кодовых слов, соответствующих информационной посылке с одним ненулевым символом в информационной последовательности. Для длины $n = 12$ выполнен полный перебор кодовых слов.

Следует отметить, что при уменьшении на одну генераторную функцию при построении алгеброгеометрических кодов на пространственных кривых Артин-Шраера над $GF(4)$ удается построить кодовые конструкции с параметрами (12, 8, 3) и (12, 3, 8), что дает лучший по сравнению с кодом БЧХ (12, 3, 7) результат.

Таблица 1 - Экспериментальная оценка кодовых соотношений алгеброгеометрических кодов на пространственныхкривых Артин-Шраера

$\deg F$	k	d		$k_\perp$	$d_\perp$
$\begin{cases} f_1(x_0,x_1,x_2,x_3) = x_0x_1^2 + x_1x_2^2 - x_0^2x_2 = 0 \\ f_2(x_0,x_1,x_2,x_3) = x_1x_2^2 + x_2x_3^2 - x_1^2x_3 = 0 \end{cases}$, $g = 5$, $n = 12$ над $GF(4)$;					
1	4	6		8	2
2	10	2		2	8
$\begin{cases} f_1(x_0,x_1,x_2,x_3) = x_0^3x_1^4 + x_1x_2^6 - x_0^4x_2^3 = 0 \\ f_2(x_0,x_1,x_2,x_3) = x_1^3x_2^4 + x_2x_3^6 - x_1^4x_3^3 = 0 \end{cases}$, $g = 57$, $n = 240$ над $GF(16)$;					
1	4	216		236	3
2	10	200		230	4
3	20	184		220	8
5	35	172		205	14
6	56	148		184	32
7	84	100		156	65
8	116	68		124	80
9	150	56		90	96
10	183	36		57	132

Анализ полученных экспериментальных результатов (см. таблицу 1) позволяет сделать вывод об их сходимости с теоретическими оценками кодовых соотношений алгеброгеометрических кодов на пространственных кривых Артин-Шраера, что подтверждает достоверность полученных результатов.

ВЫВОДЫ

1 Построение эффективных помехоустойчивых кодов в общетеоретическом плане сопряжено с построением длинных (с большим n) блоковых кодов, сохраняющих высокие конструктивные кодовые соотношения (n, k, d). Эта задача в терминах алгеброгеометрических кодов формулируется в виде задачи поиска регулярных методов построения линейных систем, возникающих на алгебраических кривых с

большим числом точек N, по отношению к роду кривой g. В результате проведенных исследований обоснован выбор обобщенной конструкции Артин-Шраера как реального источника кривых для построения эффективных помехоустойчивых кодов.

2 В результате проведенных исследований получены оценки кодовых соотношений алгеброгеометрических кодов, построенных на пространственных кривых Артин-Шраера. Анализ полученных зависимостей показывает, что практически с увеличением длины кода и мощности алфавита кодовых символов алгеброгеометрические коды лежат выше нижней теоретической границы Варшамова-Гилберта и дают лучший по сравнению с недвоичными БЧХ-кодами результат.

3 Приведенные экспериментальные оценки кодовых соотношений алгеброгеометрических кодов на пространственных кривых показали сходимость результатов эксперимента с теоретическими оценками, что подтверждает достоверность полученных результатов.

SUMMARY

THE CONSIDERATION OF ALGEBRAIC – GEOMETRY CODES ON ARTIN-SCHRAIER SPATIAL CURVES FOR THE INCREASING OF NOISE STABILITY OF DISCRETE MESSAGES TRANSMISSIONS

N.N. Lyapa, V.I. Grabchak, I.V.Pasko

Noise stability of discrete messages transmissions with the use of algebraic- geometry codes on Artin-Schraier spatial curves are considered.

СПИСОК ЛИТЕРАТУРЫ

1. Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т.259. – № 6. – С. 1289 –1290.
2. Кузнецов А.А. Энергетический выигрыш алгеброгеометрического кодирования //Всеукр. меж вед. науч.-техн. сб. – Харьков: ХТУРЭ, 2003. – Вып.134. – С. 218 –222.
3. Кузнецов А.А. Энергетическая эффективность алгеброгеометрических кодов //Электронное моделирование: Международный научно-теоретический журнал. – К.: НАНУ, РАН, 2004. – № 2. – С. 27 –38.
4. Науменко М.І., Стасєв Ю.В., Кузнецов О.О. Теоретичні основи побудови алгебраїчних кодів: Монографія. – Харків: ХУПС, 2005. – 267 с.
5. Кузнецов А.А., Пасько И.В. Алгеброгеометрические коды на пространственных кривых // Матеріали першої науково-технічної конференції "Науково-методичні основи оцінювання та управління техногенною безпекою у разі виникнення надзвичайної ситуації": Програма конференції та тези доповідей. – Харків: НДІ макрографії. – 2007. – С. 8 –9.
6. Шеннон К. Работы по теории информации и кибернетике. – М.: ИЛ. – 1963. – 829 с.
7. Кузнецов А.А., Ушно С.В. Поиск неприводимых алгебраических кривых малой степени в конечных полях // Системи обробки інформації. – Харків: НАНУ, ПАНИ, ХВУ. – 2004. – С. 147 –150.
8. Ian Blake, Chris Heegard, Tom Hoholdt, Victor K. W. Wei. Algebraic – Geometry Codes, IEEE Trans. Info. Theory, October 1998. – Vol. IT-44. – P. 2596 –2618.

Н.Н. Ляпа, канд. техн. наук, доцент Военного института РВиА СумГУ, г. Сумы;
В.И. Грабчак, канд. техн. наук, доцент Военного института РВиА СумГУ, г. Сумы;
И.В. Пасько, научный сотрудник Военного института РВиА СумГУ, г. Сумы

Поступила в редакцию 29 августа 2007 г.