УДК 681.3

**Івчук Д.О.**

# ОСОБЛИВОСТІ АЛГЕБРАЇЧНОГО ДЕКОДУВАННЯ НА ПРОСТОРОВИХ КРИВИХ

Вінницький національний технічний університет

***Анотація***

*Розглянуто та запропоновано алгоритм алгебраїчного декодування на просторових кривих для ефективного захисту від помилок в телекомунікаційних системах.*

**Ключові слова:** кодування, алгеброгеометричне кодування, просторові криві.

***Annotation***

*An algorithm for algebraic decoding on spatial curves is considered and proposed for effective protection against errors in telecommunication systems.*

**Key words:** coding, algebra geometric coding, spatial curves.

## Вступ

Одним з ефективних засобів захисту інформації від помилок в телекомунікаційних системах є завадостійке кодування інформації [1]. Основними вимогами до завадостійкого кодування є висока виявляє і виправляє здатність коду, низька яку вносить надмірність, високу швидкодію і низька складність реалізації процедур кодування-декодування [2]. Недвійкові алгебраїчні блокові коди, побудовані по алгебраїчним кривим, мають високу виправляючу здатність при невеликій частці вносимої надлишковості. У той же час методи декодування алгеброгеометричних кодів орієнтовані на вузький клас кодів і, строго кажучи, не дозволяють реалізувати їх потенційні властивості.

## Результати дослідження

Алгоритм декодування алгеброгеометричних кодів визначимо як послідовність наступних кроків.

КРОК 1. За виразом обчислимо елементи синдромної послідовності.

КРОК 2. Вирішимо систему лінійних рівнянь. Отримаємо коефіцієнти многочлена локаторів помилок.

КРОК 3. Скористаємося процедурою Ченя. Стосовно до декодування алгеброгеометричних кодів на просторових кривих вона складається підстановці всіх пар (Xi, Yi, Zi), відповідних проектних точках просторової кривої, в многочлен локаторів помилок. Ті пари, які при підстановці в цей многочлен звертають його в нуль, локалізують помилки, тобто вказують на їх шукане розташування.

КРОК 4. Підставляємо отримані локатори помилок в систему рівнянь c * H = 0. Рішення системи лінійних рівнянь дасть значення (кратність) відбулися помилок. локалізація помилок і знайдені їх значення дозволяють сформувати вектор помилок e = (e 0, e1, ..., en-1).

КРОК 5. Виправимо помилки: c = c* - e. Оцінимо складність реалізації запропонованого алгоритму декодування. Основні етапи розробленого алгебраїчного алгоритму полягають у вирішенні системи лінійних рівнянь (кроки 2 і 4) і виконанні процедури Ченя (крок 3). Ці стандартні процедури, а також процедура обчислення вектора синдромів можуть бути реалізовані будь-яким з відомих на сьогоднішній день алгоритмів. Складність рішення системи лінійних рівнянь методом Гаусса O ($n^2$), де n - число змінних. В системі (6) число рівнянь відповідає числу одночленним від трьох невідомих ступеня (t - 2), отже, число рівнянь можна висловити виразом:

$$\frac{(t+1)!}{(t-2)!(t+1-(t-2))} = \frac{(t+1)(t)(t-1)}{3} = \frac{t^3-t}{3}.$$

Таким чином, складність реалізації 2-го кроку алгоритму становить:

$$\left(\frac{(t^3-t)}{3}\right)^2 = \frac{(t^6-2t^4+t^2)}{3}.$$

Складність реалізації процедури Ченя становить 6(t – 2). Загальна складність алгоритму

$$\frac{(t^6-2t^4+54t-108)}{9},$$

асимптотична складність (в межі як функція розміру завдання): $O(t) = t^6 – t^4 + t^2 + t$.

## Висновки

Розроблений практичний алгоритм декодування алгеброгеометричних кодів на просторових кривих, заснований на зведенні завдання декодування до вирішення систем лінійних рівнянь. Складність його реалізації зростає поліноміально від параметрів коду.

## Список використаної літератури

1.Касаткина, Ю. ␣С. Анализ рода кривой, соответствующей подкоду наименьшего веса рационального кода Гоппы / Ю. ␣С. Касаткина, А. ␣С. Касаткина // Вестник Волгоградского государственного университета. Серия 1, Математика. Физика. — 2014. — № 4 (23). — С. 6–10.

2. Ruud Pellikaan. Asymptotically good sequences of curves and codes. // Proc. 34th Allerton Conf. on Communication, Control, and Computing, Urbana-Champaign, October 2-4, 2006. – P. 276-278.

***Івчук Дмитро Олегович –*** студент факультету менеджменту та інформаційної безпеки, Вінницький національний технічних університет, Вінниця.

Науковий керівник: ***Шиян Анатолій Антонович*** - канд. техн. наук, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет.

***Dmytro Ivchuk*** - student of the Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia.

Scientific adviser: ***Anatoliy Shiyan*** - cand. tech. Sciences, Associate Professor, Department of Management and Security of Information Systems, Vinnitsa National Technical University.