**УКРАЇНСЬКАЯ ДЕРЖАВНА АКАДЕМІЯ
ЗАЛІЗНИЧНОГО ТРАНСПОРТУ**

Пасько Ігор Володимирович

УДК 621.391.25.019.4 (0.43)

МЕТОДИ ПОБУДОВИ ЛІНІЙНИХ БЛОКОВИХ КОДІВ З ПОКРАЩЕНИМИ ВЛАСТИВОСТЯМИ ДЛЯ ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ ПЕРЕДАЧІ ДИСКРЕТНИХ ПОВІДОМЛЕНЬ

Спеціальність: 05.12.02 - телекомунікаційні системи і мережі

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків-2008

Дисертацією є рукопис.

Робота виконана у Харківському університеті Повітряних Сил імені Івана Кожедуба Міністерство оборони України

Науковий керівник – кандидат технічних наук, старший науковий співробітник
Кузнецов Олександр Олександрович
Харківський університет Повітряних Сил ім. Івана Кожедуба, начальник інформаційно-обчислювального центру – старший науковий співробітник

Офіційні опоненти: доктор технічних наук, професор
Сорока Леонід Степанович,
Харківський національний університет імені В.Н. Каразіна, декан факультету комп'ютерних наук

кандидат технічних наук, доцент,
Сумцов Дмитро Вікторович,
Харківський університет Повітряних Сил ім. Івана Кожедуба, заступник начальника кафедри математичного та програмного забезпечення АСУ

Захист відбудеться "___"_____2008р. о _____ годині на засіданні спеціалізованої Вченої Ради Д64.820.01 у Українській державній академії залізничного транспорту за адресою: 61050 м. Харків, майдан Фейєрбаха, 7

З дисертацією можна ознайомитись у бібліотеці Української державної академії залізничного транспорту

Автореферат розісланий "___"_____2008р.

Вчений секретар
Спеціалізованої вченої ради Приходько С.І.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Одним із головних стратегічних пріоритетів державної політики України у сфері науки і техніки є розвиток перспективних інформаційних технологій, приладів автоматизації і систем зв’язку. Відповідно до Закону України "Про Концепцію Національної програми інформатизації" одним із основних напрямків інформатизації є інформатизація стратегічних напрямків розвитку державності, безпеки і оборони. Головною особливістю завдань цього напрямку є висока складність, обумовлена високими вимогами до швидкості та форми надання інформації, завадостійкості і безпеки передачі дискретних повідомлень у телекомунікаційних системах і мережах.

Основними і найбільш ефективними засобами підвищення завадостійкості передачі дискретних повідомлень є методи завадостійкого кодування. Найбільшого розвитку серед них набули методи та алгоритми побудови алгебраїчних блокових кодів, зокрема, циклічних кодів. Поряд з високими конструктивними властивостями циклічних кодів цей напрямок дозволяє будувати прості і обчислювально ефективні алгоритми кодування та декодування. У той же час їх практичне використання при великій довжині кодового слова (> 1000 символів) не дозволяє суттєво підвищити енергетичну ефективність передачі дискретних повідомлень. Це пояснюється, перш за все, незадовільними асимптотичними властивостями циклічних кодів.

Теоретичним узагальненням алгебраїчних кодів, які допускають поліноміальний опис многочленами від однієї формальної змінної, є коди, асоційовані з алгебраїчними кривими (алгеброгеометричні коди). Асимптотично алгеброгеометричні коди за своїми параметрам перебувають вище нижньої кодової границі Варшамова-Гілберта. На сьогоднішній день методи побудови та декодування алгеброгеометричних кодів досліджені для плоских алгебраїчних кривих, що дозволяє будувати прості схеми кодування та декодування невеликої довжини. Перспективним напрямком у цьому розумінні є розробка методів побудови алгеброгеометричних кодів на просторових кривих. Вирішення цього завдання дозволить будувати довгі недвійкові блокові коди, з кодовими характеристиками, що перебувають вище границі Варшамова-Гілберта. Їх практичне використання дозволить підвищити енергетичну ефективність передачі дискретних повідомлень, що при фіксованій імовірності помилкового прийому символів повідомлення дозволить суттєво знизити вимоги до мінімально необхідного співвідношення енергії сигналу до спектральної щільності шуму, тобто підвищити завадостійкість передачі дискретних повідомлень.

Таким чином, розвиток методів та алгоритмів побудови алгеброгеометричних кодів на просторових кривих є перспективним напрямком досліджень, який має важливе значення як для розвитку окремого напрямку теорії завадостійкого кодування, так і для вирішення прикладних питань завадостійкої передачі повідомлень каналами із випадково виникаючими помилками. Тому тема дисертаційного дослідження є актуальною.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження в дисертаційній роботі проводилися відповідно до наступних нормативних актів: Концепція розвитку зв’язку України до 2010 року, затверджена постановою Кабіне-

ту Міністрів України «Про Концепцію розвитку зв'язку України до 2010 року» від 9 грудня 1999 р. №2238; Концепція Національної програми інформатизації схваленої Законом України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 р. № 75/98-ВР; державна науково-технічна програма «Створення перспективних телекомунікаційних систем і технологій»; тактико-технічне завдання на науково-дослідні роботи:

1. «Розробка методів підвищення якості військового зв'язку автоматизованої системи управління ракетних військ і артилерії», шифр «Мрія», ДР № 0101U000414.
2. Тактико-технічне завдання на науково-дослідну роботу на спеціальну тему, шифр «Облік», ДР № 0101U000668.
3. Тактико-технічне завдання на дослідно-конструкторську роботу «Створення УКХ радіостанцій, що забезпечують енергетично скритний та завадостійкий радіозв'язок у повнозв'язаній мережі».

Мета дисертаційних досліджень.

Метою дисертаційної роботи є підвищення завадостійкості передачі дискретних повідомлень на основі використання лінійних блокових кодів з покращеними властивостями. Відповідно до мети роботи необхідно вирішити **наукове завдання**, яке полягає в розробці методів і алгоритмів побудови лінійних блокових кодів з покращеними властивостями для підвищення завадостійкості передачі дискретних повідомлень.

Для досягнення цієї мети необхідно вирішити наступні **завдання.**

1. Провести аналіз стану та обґрунтувати шляхи розвитку методів кодування для підвищення завадостійкості передачі дискретних повідомлень.
2. Розробити метод і алгоритми завадостійкого кодування алгеброгеометричними кодами на просторових кривих для підвищення завадостійкості передачі дискретних повідомлень.
3. Розробити алгебраїчний метод и алгоритм декодування алгеброгеометричних кодів на просторових кривих для підвищення завадостійкості передачі дискретних повідомлень.
4. Оцінити завадостійкість передачі дискретних повідомлень з використанням алгеброгеометричних кодів на просторових кривих.

Об'єкт дослідження - процес завадостійкої передачі дискретних повідомлень каналами із випадково виникаючими помилками.

Предмет дослідження - методи побудови лінійних блокових кодів з покращеними властивостями для підвищення завадостійкості передачі дискретних повідомлень.

Методи дослідження. При розробці методів і алгоритмів побудови та декодування лінійних блокових кодів з покращеними властивостями використані методи алгебраїчної теорії блокових кодів і теорії інформації, а також методи теорії алгебраїчних кривих і теорії кінцевих полів Галуа. При розробці практичних пропозицій з апаратної реалізації алгоритмів кодування і декодування використано методи теорії автоматів і теорії складності. При дослідженні завадостійкості передачі дискретних повідомлень використано методи статистичної теорії зв'язку, теорії ймовірності і математичної статистики.

Наукова новизна отриманих результатів обумовлена теоретичним узагальненням і новим вирішенням науково-технічного завдання, що полягає в розробці методів і алгоритмів побудови лінійних блокових кодів з покращеними властивостями для підвищення завадостійкості передачі дискретних повідомлень.

Отримано такі **наукові результати**.

Вперше одержано нові кодові конструкції завадостійких кодів як лінійних систем, що виникають на просторових кривих, які відрізняються від відомих тим, що при фіксованій потужності алфавіту символів та без погіршення кодових співвідношень вдається побудувати лінійні блокові коди більшої довжини [4, 6, 8].

Дістали подальшого розвитку методи завадостійкого кодування недвійковими блоковими кодами, що виникають на алгебраїчних кривих. Розроблено метод кодування алгеброгеометричними кодами на просторових кривих, який відрізняється від відомих формуванням базису лінійного коду через відображення множини спільних рішень двох однорідних алгебраїчних рівнянь від чотирьох змінних, що дозволяє при фіксованій потужності алфавіту символів та при збереженні високих конструктивних кодових характеристик отримати більшу довжину коду [3, 6].

Удосконалено методи декодування недвійкових блокових кодів, що виникають на алгебраїчних кривих. Розроблено алгебраїчний метод декодування алгеброгеометричних кодів на просторових кривих, який відрізняється від відомих формуванням триваріантного рівняння локаторів помилок, рішення якого однозначно задаються помилками, які виникають, що дозволяє звести задачу декодування до вирішення системи лінійних рівнянь, у яких число невідомих визначається конструктивними кодовими характеристиками [1, 5, 7].

Практичне значення результатів досліджень полягає в такому.

Розроблені практичні рекомендації щодо реалізації запропонованих методів завадостійкого кодування алгеброгеометричними кодами на просторових кривих. Розроблено алгоритми та структурні схеми пристроїв завадостійкого кодування алгеброгеометричними кодами на просторових кривих. Показано, що формування кодових слів реалізується з використанням елементарних арифметичних операцій над елементами кінцевого поля та може бути виконано алгоритмами поліноміальної складності від параметрів коду. Формально асимптотична ємкісна складність кодування (n, k, d) кодами оцінюється як $O(n)$, асимптотична часова складність оцінюється як $O(kn)$ та $O((n-k)n)$ [3, 6].

Розроблено алгоритм та структурну схему пристрою алгебраїчного декодування алгеброгеометричними кодами на просторових кривих. Показано, що складність алгебраїчного декодування запропонованим методом росте поліноміально від виправляючої спроможності коду. Обґрунтовано доцільність реалізації розроблених декодерів на сучасній обчислювальній техніці при виправляючій спроможності коду $t \leq 100$ [1, 8, 10].

Досліджено завадостійкість передачі дискретних повідомлень з використанням алгеброгеометричних кодів на просторових кривих. Показано, що при фіксованій потужності алфавіту символів та довжині застосування алгеброгеометричних кодів на просторових кривих дозволяє отримати енергетичний виграш від кодування *0,5-0,8 дБ* порівняно з недвійковими кодами БЧХ [4].

Отримані результати використано в науково-дослідних роботах, що проводяться в рамках Державної науково-технічної програми «Створення перспективних телекомунікаційних систем і технологій». Отримано акти впровадження результатів досліджень при проведенні науково-дослідних робіт та на виробництві.

Публікації. Основні результати досліджень опубліковані в шести наукових статтях. **Особистий внесок автора** дисертації в статті, виконані у співавторстві, полягає в наступному: у [2] автором проведено аналіз математичної моделі та структурної схеми систем передачі даних у телекомунікаційних системах і мережах; у [3] автором розроблені практичні алгоритми кодування алгеброгеометричними кодами на просторових кривих в систематичному і несистематичному виді. Оцінена складність їх реалізації; у [4] автором проводяться дослідження завадостійкості передачі дискретних повідомлень у телекомунікаційних системах з використанням алгеброгеометричних кодів на просторових кривих у каналах з незалежним розподілом помилок; у [5] автором отримано аналітичні вирази для проведення декодування алгеброгеометричних кодів за кривими в P^3, які дозволяють звести задачу декодування до вирішення систем лінійних рівнянь, у яких число невідомих задається конструктивними кодовими характеристиками. Показано, що складність алгебраїчного декодування методом, що пропонується, росте поліноміально від виправляючої спроможності коду; у [6] автором досліджується загальна конструкція алгеброгеометричних кодів як лінійних систем, що виникають на проективних алгебраїчних кривих. Розроблено метод і алгоритми завадостійкого кодування алгеброгеометричними кодами, які задані на просторових кривих.

Апробація результатів дисертації. Основні результати досліджень доповідалися та були схвалені на чотирьох науково-технічних конференціях: Міжнародна науково-технічна конференція „Інтегровані комп'ютерні технології в машинобудуванні" ІКТМ-2006 (Харків, 2006) [7]; Третя міжнародна наукова конференція „Современные методы кодирования в электронных системах" СМКЭС-2006 (Суми, 2006) [8]; Перша науково-технічна конференція «Науково-методичні основи оцінювання та управління техногенною безпекою у разі виникнення надзвичайної ситуації» (Харків, 2007) [9]; Третя наукова конференція Харківського університету Повітряних Сил ім. Івана Кожедуба (Харків, 2007) [10].

Структура дослідження. Дисертація складається зі вступу, чотирьох розділів, висновків, переліку використаних джерел і додатків. Повний обсяг дисертації 174 сторнки, рисунків – 15, таблиць – 3. Бібліографія із 130 найменувань на 12 сторінках. 2 додатки загальним обсягом 38 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовується вибір теми та її актуальність, визначаються об'єкт та предмет дослідження, мета та завдання роботи, методи дослідження. Зазначено наукову новизну результатів дисертаційного дослідження, вказано теоретичне та практичне значення здобутих результатів.

У першому розділі проводиться аналіз структурної схеми і математичної моделі системи передачі дискретних повідомлень, досліджуються критерії і

показники

якості передачі даних. Аналізується стан і обґрунтовуються шляхи розвитку методів завадостійкого кодування, обґрунтовується вибір напрямку досліджень та математично формалізується постановка наукової задачі.

Математична модель і структурна схема системи передачі даних складається з наступних елементів (рис. 1.): 1) ДП - джерело повідомлень; 2) АКДІ - апаратура кодування джерела інформації; 3) АКК - апаратура канального (завадостійкого) кодування; 4) ПРД - передавач повідомлень, що перетворює за деяким правилом інформаційні повідомлення в сигнали, що відповідають характеристикам даного каналу; 5) канал – середовище, що використовується для передачі сигналу від джерела до приймача; 6) ПРМ - приймач, що виконує операцію, зворотну стосовно операції, виробленої передавачем; 7) АД - апаратура декодування, що виконує операції, зворотні канальному кодуванню (декодер завадостійкого коду); 8) АДОІ - апаратура декодування одержувача інформації; 9) ОІ - одержувач інформації.

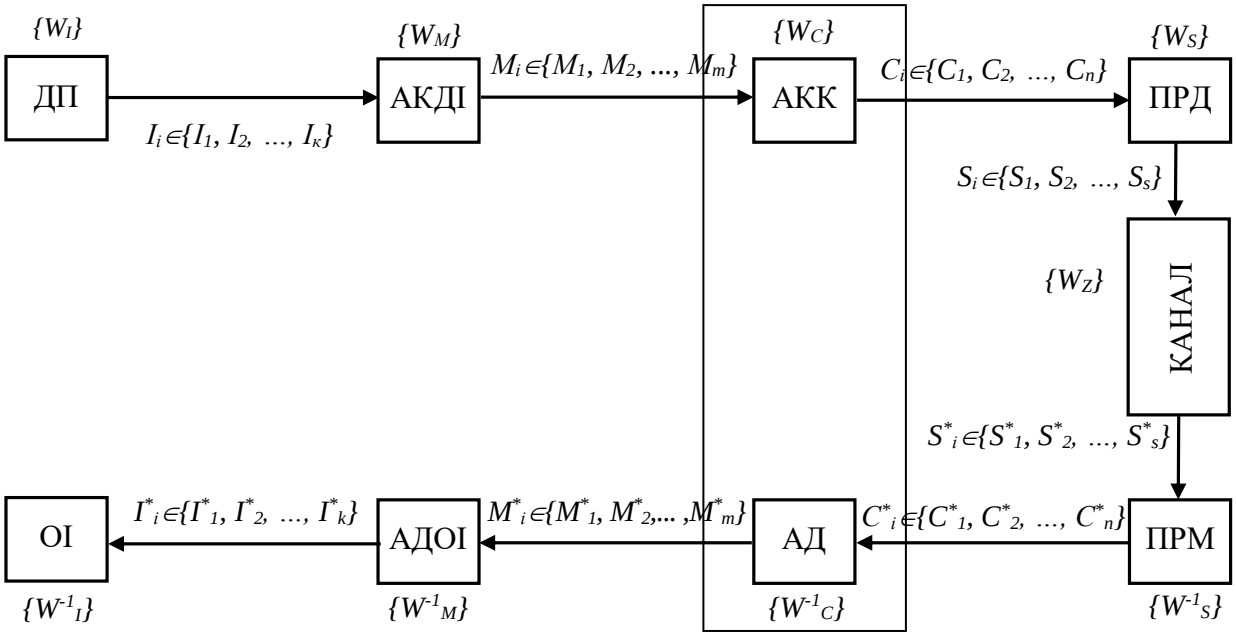


Рис. 1. Математична модель і структурна схема системи передачі даних.

На рис. 1 позначені: $\{W_I\}$ – оператор формування інформаційних повідомлень; $\{W_M\}$ – оператор перетворення інформаційних повідомлень в інформаційні блоки даних (оператор кодування джерела); $\{W_C\}$ – оператор перетворення інформаційних блоків даних у кодові слова (оператор завадостійкого кодування); $\{W_S\}$ – оператор перетворення кодових слів у послідовність сигналів (оператор формування сигналів); $\{W_Z\}$ – оператор взаємодії переданих сигналів з навмисними й ненавмисними перешкодами в каналі зв'язку; $\{W^{-1}_S\}$ – оператор перетворення послідовності сигналів у кодове слово (оператор обробки сигналів); $\{W^{-1}_C\}$ – оператор перетворення кодових слів у інформаційні блоки даних (оператор декодування завадостійкого коду); $\{W^{-1}_M\}$ – оператор перетворення інформаційних блоків даних в інформаційні повідомлення (оператор декодування одержувача інформації); $\{W^{-1}_I\}$ – оператор обробки отриманих повідомлень.

Аналіз структурної схеми й математичної моделі системи передачі даних показує, що формальний опис системи завадостійкого кодування задається сукупністю наступних операторів: оператора перетворення інформаційних блоків даних у кодові слова (оператор завадостійкого кодування) $\{W_C\}$, оператора перетворення кодових слів у інформаційні блоки даних (оператор декодування завадостійкого коду) $\{W^{-1}_C\}$. Апаратура канального (завадостійкого) кодування реалізує відображення безлічі інформаційних блоків даних $\{M_1,M_2,...,M_m\}$ у безліч кодових слів $\{C_1, C_2, ..., C_n\}$. Метою завадостійкого кодування є внесення за певним алгоритмом у передані дані надлишковості. На прийомній стороні, аналізуючи прийняті кодові слова з можливою помилкою $C^*_i \in \{C^*_1,C^*_2,...,C^*_n\}$ і їх відповідність внесеній надлишковості, апаратура завадостійкого декодування зменшує дію виниклих при передачі повідомлень помилок.

Під завадостійкістю розуміють властивість зв'язку, що характеризує її здатність забезпечувати передачу повідомлень із заданою ймовірністю помилки в умовах взаємодії перешкод усіх видів. Кількісною мірою завадостійкості є γ – мінімальне співвідношення енергії сигналу до спектральної щільності потужності шуму, необхідне для забезпечення необхідної ймовірності. Основним показником оцінки ймовірності є ймовірність правильного прийому $P_{n.n.}$, показником втрати ймовірності є зворотна величина $P_{пом}$ – імовірність перекручування символів повідомлення в процесі передачі. Таким чином, цільову функцію підвищення завадостійкості можна записати у вигляді функціонала

$$\Psi(\gamma, P_{пом}) = \langle min(\gamma), P_{пом} = const \rangle .$$

У другому розділі розглядаються основні положення алгебраїчної геометрії, необхідні для конструювання алгеброгеометричних кодів, вводяться основні терміни й визначення. Досліджується загальна конструкція алгеброгеометричних кодів, як лінійних систем, що виникають на проективних алгебраїчних кривих. Розробляється метод і практичні алгоритми завадостійкого кодування алгеброгеометричними кодами, заданими на просторових кривих.

Зафіксуємо гладку проективну алгебраїчну криву X роду g у проективному просторі P^3 над полем $GF(q)$ як сукупність рішень двох однорідних незвідних алгебраїчних рівнянь від 4-х змінних з коефіцієнтами з $GF(q)$

$$\begin{cases} f_1(x_0,x_1,x_2,x_3) = 0 \\ f_2(x_0,x_1,x_2,x_3) = 0 \end{cases}. \qquad (1)$$

Нехай $p_0(x_0,x_1,x_2,x_3)$, $p_1(x_0,x_1,x_2,x_3)$, …, $p_{N-1}(x_0,x_1,x_2,x_3)$ – N спільних рішень системи рівнянь (1) – точок просторової кривої X.

Зафіксуємо дивізор D кривої X і множену раціональних функцій, асоційованих з дивізором D, тобто множену, що складається з нуля й функцій $f \neq 0$, для яких $(f) + D \geq 0$. Це еквівалентно набору генераторних функцій $F_0(x_0,x_1,x_2,x_3)$, $F_1(x_0,x_1,x_2,x_3)$, …, $F_m(x_0,x_1,x_2,x_3)$, де $F_0, F_1,...,F_m$ - форми однакового ступеня і $F_0(x_0,x_1,x_2,x_3) \neq 0$.

Нехай α – степінь класу дивізорів, $\alpha > g-1$, тоді відображення $\varphi: X \to P^m$ задає породжуючу матрицю G алгеброгеометричного коду з конструктивними характеристиками $(n \le N, k \ge \alpha - g + 1, d \ge n - \alpha)$.

Визначення 1 [3, 6, 9]. Алгеброгеометричний код на просторовій кривій *X* над *GF(q)*, побудований через породжуючу матрицю *G* - це лінійний код, всі кодові слова $(c_0, c_1, \ldots, c_{n-1})$ якого задаються рівністю

$$\sum_{i=0}^{m-1} I_i F_i\left(p_j(x_0, x_1, x_2, x_3)\right) = c_j, \ j = 0,\ldots,n-1.$$

Для формування кодового слова $(c_0, c_1, \ldots, c_{n-1})$ через породжуючу матрицю достатньо для всіх $j = 0,\ldots,n-1$ виконати перетворення:

$$c_j = \sum_{i=0}^{m-1} I_i F_i\left(p_j(x_0, x_1, x_2, x_3)\right).$$

Нехай $\alpha > 2g-2$, тоді відображення $\varphi: X \to P^{m-1}$ задає перевірочну матрицю *H* алгеброгеометричного коду, з конструктивними характеристиками $(n \le N, k \ge n - \alpha + g - 1, d \ge \alpha - 2g + 2)$.

Визначення 2 [3, 6, 9]. Алгеброгеометричний код по кривій *X* над *GF(q)* побудований через перевірочну матрицю *H* – це лінійний код, що складається з всіх слів $(c_0, c_1, \ldots, c_{n-1})$ довжини $n \le N$, для яких виконується рівність *d + g - 1* рівнянь

$$\sum_{i=0}^{n-1} c_i F_j\left(p_i(x_0, x_1, x_2, x_3)\right) = 0, \quad j = 0,\ldots,m. \qquad (2)$$

Для формування кодових слів розіб'ємо слово $(c_0, c_1, \ldots c_{n-1})$ на множину інформаційних і перевірочних позицій. Нехай *U* - множина *k* інформаційних позицій кодового слова (тобто множина номерів позицій, що входять до заданого інформаційного набору коду) і *W* - множину *r= n-k* перевірочних позицій. Об'єднання множин $U \cup W$ містить всі цілі числа (номери) від 0 до n-*1*. На *k* інформаційних позиціях множини *U* розмістимо *k* символів повідомлення $(I_0, I_1, \ldots I_{k-1})$, а на перевірочних позиціях множини *W* розмістимо *r* нульових символів. Обчислимо суми

$$S_j = \sum_{i=0}^{n-1} c_i F_j\left(p_i(x_0, x_1, x_2, x_3)\right), \ j = \overline{0, r-1}.$$

Завдання формування кодового слова полягає в тому, щоб обчислити й записати на $r = n - k$ перевірочних позиціях такі символи c_i, $i \in W$, які задовольняють рівнянням (2). З визначення 2 витікає, що значення *r* перевірочних символів можуть бути знайдені із системи лінійних рівнянь

$$\sum_{i \in W} c_i F_j\left(p_i(x_0, x_1, x_2, x_3)\right) = -S_j, \ j = \overline{0, r-1}.$$

Використовуючи методи обертання матриць, запишемо

$$\|c_i\|_r = \left\|F_j\left(p_i(x_0, x_1, x_2, x_3)\right)\right\|_{r,r}^{-1} \left\|-S_j\right\|_r^T,$$

Для формування кодового слова алгеброгеометричного коду на просторових кривих через перевірочну матрицю досить зберігати елементи матриць $\left\|F_j\left(p_i\left(x_0,x_1,x_2,x_3\right)\right)\right\|_{k,r}$ і $\left\|F_j\left(p_i\left(x_0,x_1,x_2,x_3\right)\right)\right\|_{r,r}^{-1}$ або по черзі обчислювати їх як значення генераторних функцій у точках просторової кривої.

Розглянуті операції дозволяють формувати кодові слова алгеброгеометричних кодів на просторових кривих, заданих як через породжуючу, так і через перевірочну матриці. На рис. 2 представлено схеми пристроїв завадостійкого кодування алгеброгеометричними кодами на просторових кривих: а) структурна схема пристрою завадостійкого кодування через породжуючу матрицю; б) структурна схема пристрою завадостійкого кодування через перевірочну матрицю: БВІ - блок введення інформаційної послідовності; БУ - блок узгодження; БЗТ - блок зберігання точок просторової кривої; БЗФ - блок зберігання генераторних функцій; ВБ1 - 1-й вирішуючий блок (обчислення значень генераторних функцій у точках просторової кривої); ВБ2.а) - 2-й вирішуючий блок (обчислення елементів кодового слова); ВБ2.б) – 2-й вирішуючий блок (обчислення елементів вектора $\left(S_0,S_1,...S_{r-1}\right)$); ВБ3 – 3-й вирішуючий блок (обчислення перевірочних символів кодового слова); БФКС – блок формування кодового слова.

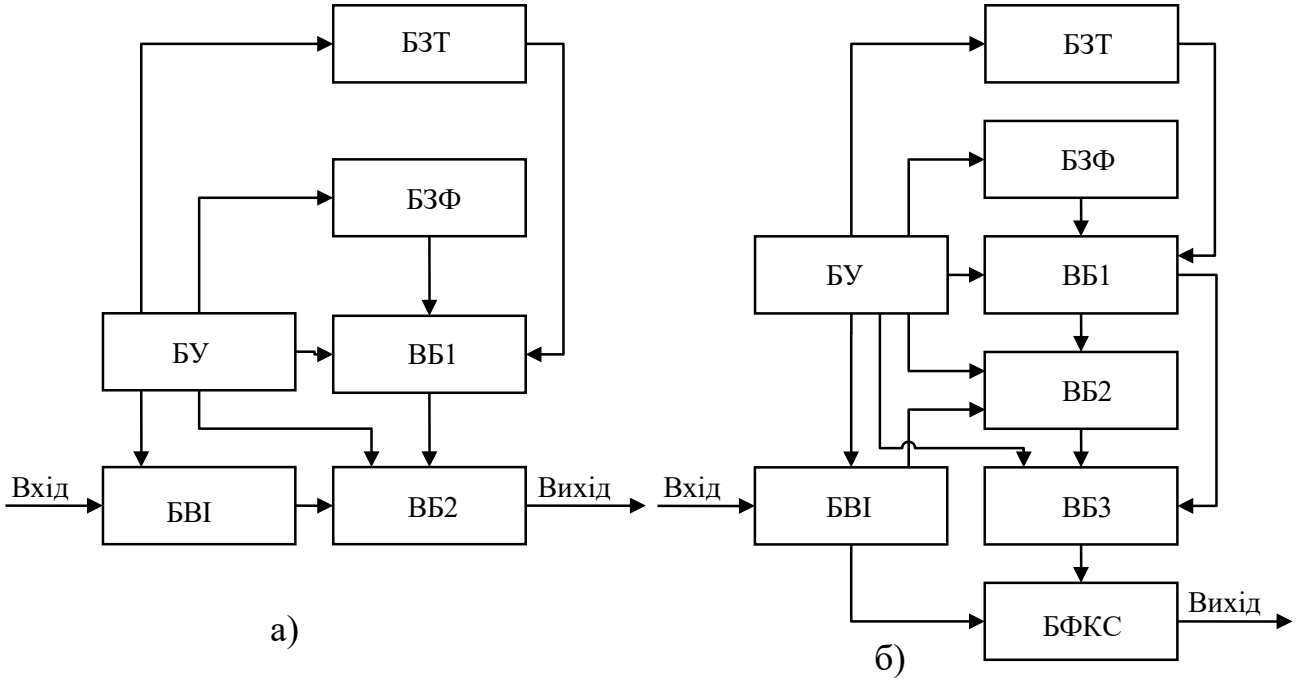


Рис. 2. Структурна схема пристрою завадостійкого кодування алгеброгеометричними кодами на просторових кривих

Розроблені структурні схеми пристроїв дозволяють реалізувати запропоновані алгоритми завадостійкого кодування алгеброгеометричними кодами на просторових кривих через породжуючу та перевірочну матриці і практично використовувати розроблений метод для завадостійкої передачі дискретних повідомлень каналами з помилками.

У третьому розділі досліджуються методи декодування алгеброгеометричних кодів. Розглядаються алгебраїчні процедури, що складаються в зведенні задачі

декодування алгеброгеометричних кодів до розв'язання системи лінійних рівнянь із невідомими коефіцієнтами многочлена локаторів помилок від декількох змінних. Пропонується алгебраїчний метод декодування алгеброгеометричних кодів, що узагальнює постановку й рішення задачі декодування кодів заданих на просторових кривих. Розробляється алгоритм декодування, що практично реалізує пропонований метод, досліджується його ємкісна і часова складність реалізації.

Розглянемо кодове слово алгеброгеометричного *(n, k, d)* коду над *GF(q)*, побудованого по просторових кривих. Припустимо, що алгеброгеометричний код заданий через перевірочну матрицю

$$H = \begin{pmatrix} F_{0,0,0}(X_0,Y_0,Z_0) & F_{0,0,0}(X_1,Y_1,Z_1) & \dots & F_{0,0,0}(X_{n-1},Y_{n-1},Z_{n-1}) \\ F_{1,0,0}(X_0,Y_0,Z_0) & F_{1,0,0}(X_1,Y_1,Z_1) & \dots & F_{1,0,0}(X_{n-1},Y_{n-1},Z_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{0,0,\deg F}(X_0,Y_0,Z_0) & F_{0,0,\deg F}(X_1,Y_1,Z_1) & \dots & F_{0,0,\deg F}(X_{n-1},Y_{n-1},Z_{n-1}) \end{pmatrix},$$

де F_{i_x,i_y,i_z} – одночлен ступеня $i_x + i_y + i_z \le \deg F$, тобто $F_{i_x,i_y,i_z} = x^{i_x} \cdot y^{i_y} \cdot z^{i_z}$.

Справедлива рівність $C \cdot H^T = 0$, звідки витікає рівність:

$$\sum_{j=0}^{n-1} C_j \cdot F_{i_x,i_y,i_z}(X_j,Y_j,Z_j) = 0.$$

Припустимо, що при передачі каналами з помилками кодове слово спотворилося, вектор помилок позначимо $e = (e_0, e_1, \dots, e_{n-1})$, а прийняте з помилками слово у вигляді $C^* = (C^*_0, C^*_1, \dots, C^*_{n-1}) = C + e = (C_0 + e_0, C_1 + e_1, \dots, C_{n-1} + e_{n-1})$. Визначимо синдромну послідовність як вектор $s = (s_{0,0,0}, s_{1,0,0}, \dots, s_{0,0,\deg F})$:

$$s_{i_x,i_y,i_z} = \sum_{j=0}^{n-1} e_j \cdot F_{i_x,i_y,i_z}(X_j,Y_j,Z_j),\ i = 0,\dots,M-1. \qquad (3)$$

Задача алгебраїчного декодування кодового слова алгеброгеометричного коду, побудованого по кривій у P^3, полягає у визначенні вектора $e = (e_0, e_1, \dots, e_{n-1})$ за відомою синдромною послідовністю $s = (s_{0,0,0}, s_{1,0,0}, \dots, s_{0,0,\deg F})$. Позначимо множину $e_j \neq 0$ символом *E*. Для однозначного визначення вектора помилок скористаємося штучним прийомом, що полягає у веденні багаточлена локаторів помилок

$$\Lambda(x,y,z) = x^{u-2} + a_{t-3,1,0} \cdot x^{u-3} \cdot y + \dots + a_{1,0,0} \cdot x + a_{0,1,0} \cdot y + a_{0,0,1} \cdot z + a_{0,0,0}, \qquad (4)$$

рішеннями якого є локатори – такі набори (X_ξ, Y_ξ, Z_ξ), які перетворюють на нуль багаточлен (4), причому всі $e_\xi \in E$.

Многочлен (4) однозначно задає розташування помилок у векторі $e = (e_0, e_1, \dots, e_{n-1})$, тому що однозначно вказує на його ненульові компоненти. Інакше кажучи, знаходження коефіцієнтів a_{i_x,i_y,i_z} багаточлена $\Lambda(x,y,z)$ дозволяє однозначно вказати на розташування виниклих при передачі кодового слова помилок.

Помножимо багаточлен (4) на e_j і обчислимо в точці (X_j, Y_j, Z_j), отримаємо:

$$\begin{aligned} e_j \cdot X_j^{u-2} + a_{t-3,1,0} \cdot e_j \cdot X_j^{u-3} \cdot Y_j + \dots + a_{1,0,0} \cdot e_j \cdot X_j + \\ + a_{0,1,0} \cdot Y_i + a_{0,0,1} \cdot e_j \cdot Z_j + a_{0,0,0} \cdot e_j. \end{aligned} \qquad (5)$$

Проаналізуємо отриманий вираз. Якщо $e_j \notin E$, тобто $e_j = 0$, тоді всі доданки отриманого багаточлена дорівнюють нулю, тобто маємо рівність нулю всього виразу (5). Якщо $e_j \in E$, тобто $e_j \neq 0$, тоді відповідні набори (X_j, Y_j, Z_j) перетворюють на нуль багаточлен (4) і, відповідно, багаточлен (5). Таким чином, при будь-якому значенні e_j маємо рівність нулю виразу (5). Додамо по всім $j = 0,\ldots,n-1$,отримаємо:

$$\sum_{j=0}^{n-1} e_j \cdot X_j^{u-2} + \sum_{j=0}^{n-1} a_{t-3,1,0} \cdot e_j \cdot X_j^{u-3} \cdot Y_j + \ldots + \sum_{j=0}^{n-1} a_{1,0,0} \cdot e_j \cdot X_j + \\ + \sum_{j=0}^{n-1} a_{0,1,0} \cdot e_j \cdot Y_j + \sum_{j=0}^{n-1} a_{0,0,1} \cdot e_j \cdot Z_j + \sum_{j=0}^{n-1} a_{0,0,0} \cdot e_j = 0. \quad (6)$$

Значення a_{i_x,i_y,i_z} не залежать від j, винесемо їх за знак додавання. З урахуванням введених вище позначень, значення одночлена $F_{i_x,i_y,i_z} = x^{i_x} \cdot y^{i_y} \cdot z^{i_z}$ в точці (X_j, Y_j, Z_j) прийме вигляд $F_{i_x,i_y,i_z}(X_j, Y_j, Z_j) = X_j^{i_x} \cdot Y_j^{i_y} \cdot Z_j^{i_z}$. З урахуванням останнього вираз (6) перепишеться у вигляді:

$$\sum_{j=0}^{n-1} e_j \cdot F_{u-2,0,0}(X_j, Y_j, Z_j) + a_{t-3,1,0} \cdot \sum_{j=0}^{n-1} e_j \cdot F_{u-3,1,0}(X_j, Y_j, Z_j) + \ldots + \\ + a_{1,0,0} \cdot \sum_{j=0}^{n-1} e_j \cdot F_{1,0,0}(X_j, Y_j, Z_j) + a_{0,1,0} \cdot \sum_{j=0}^{n-1} e_j \cdot F_{0,1,0}(X_j, Y_j, Z_j) + \\ + a_{0,0,1} \cdot \sum_{j=0}^{n-1} e_j \cdot F_{0,0,1}(X_j, Y_j, Z_j) + a_{0,0,0} \cdot \sum_{j=0}^{n-1} e_j \cdot F_{0,0,0}(X_j, Y_j, Z_j) = 0.$$

Але за введеним вище визначенням

$$s_{i_x,i_y,i_z} = \sum_{j=0}^{n-1} e_j \cdot F_{i_x,i_y,i_z}(X_j, Y_j, Z_j).$$

Отже, маємо:

$$s_{u-2,0,0} + a_{t-3,1,0} \cdot s_{u-3,1,0} + \ldots + a_{1,0,0} \cdot s_{1,0,0} + a_{0,1,0} \cdot s_{0,1,0} + a_{0,0,1} \cdot s_{0,0,1} + a_{0,0,0} \cdot s_{0,0,0} = 0.$$

Повернемося до розгляду багаточлена (4). Помножимо його на довільний одночлен $x^{i_x} \cdot y^{i_y} \cdot z^{i_z}$ і проведемо аналогічні міркування. За аналогією з (5) збережеться рівність нулю при будь-якому значенні e_j. Після додавання по всіх $j = 0,\ldots,n-1$ і виконання очевидних підстановок одержимо:

$$s_{i_x+u-2,i_y,i_z} + a_{t-3,1,0} \cdot s_{i_x+u-3,i_y+1,i_z} + \ldots + a_{1,0,0} \cdot s_{i_x+1,i_y,i_z} + \\ + a_{0,1,0} \cdot s_{i_x,i_y+1,i_z} + a_{0,0,1} \cdot s_{i_x,i_y,i_z+1} + a_{0,0,0} \cdot s_{i_x,i_y,i_z} = 0.$$

Виконавши відповідні перетворення для всіх $i = 0,\ldots,M-1$ отримаємо систему лінійних рівнянь:

$$\begin{cases} s_{u-2,0,0} + a_{u-3,1,0} \cdot s_{u-3,1,0} + \ldots + a_{1,0,0} \cdot s_{1,0,0} + a_{0,1,0} \cdot s_{0,1,0} + a_{0,0,1} \cdot s_{0,0,1} + a_{0,0,0} \cdot s_{0,0,0} = 0; \\ s_{u-1,0,0} + a_{u-3,1,0} \cdot s_{u-2,1,0} + \ldots + a_{1,0,0} \cdot s_{2,0,0} + a_{0,1,0} \cdot s_{1,1,0} + a_{0,0,1} \cdot s_{1,0,1} + a_{0,0,0} \cdot s_{1,0,0} = 0; \\ \ldots \\ s_{2 \cdot u-4,0,0} + a_{u-3,1,0} \cdot s_{2 \cdot u-5,1,0} + \ldots + a_{0,1,0} \cdot s_{u-2,1,0} + a_{0,0,1} \cdot s_{u-2,0,1} + a_{0,0,0} \cdot s_{u-2,0,0} = 0. \end{cases} \quad (7)$$

При числі невідомих v у многочлені локаторів помилок меншому за число елементів синдромної послідовності система лінійних рівнянь (7) має рішення. Складність її розв'язання, наприклад, методом Гауса складе v^2. Рішення системи (7) дають значення невідомих коефіцієнтів багаточлена локаторів помилок $\Lambda(x,y,z)$ (4), що у свою чергу однозначно задає значення локаторів – таких наборів (X_ξ, Y_ξ, Z_ξ), які перетворюють у нуль багаточлен (4), причому всі $e_\xi \in E$. Пошук (X_ξ, Y_ξ, Z_ξ) може бути виконаний, наприклад, почерговою підстановкою всіх (X_j, Y_j, Z_j), $j = 0,\ldots,n-1$ у багаточлен $\Lambda(x,y,z)$ і перевіркою на рівність нулю. Знайдені (X_ξ, Y_ξ, Z_ξ) локалізують помилку в кодовому слові, тобто прирівняють нулю

$n - u$ невідомих у системі (3). Так як кількість невідомих, що залишилися, $u < M$, то система (3) має рішення. Складність її розв'язання, наприклад, методом Гауса не перевищує u^2. Рішення системи (3) дає шукані (ненульові) значення вектора помилок

$e = (e_0, e_1, \ldots, e_{n-1})$, тобто завдання декодування вирішене.

На рис. 3 представлена структурна схема пристрою декодування алгеброгеометричних кодів на просторових кривих: БВКС - блок введення кодового слова з помилкою; БФСП - блок формування синдромної послідовності; БФГМ - блок формування генераторної матриці; БЗФ - блок зберігання генераторних функцій; БЗТ - блок зберігання точок просторової кривої; ВБ1 - 1-й вирішуючий блок (обчислення коефіцієнтів багаточлена локаторів помилок); БФЛ - блок формування локаторів помилок; ВБ2 - 2-й вирішуючий блок (обчислення значень кратності помилок); БФВП - блок формування вектора помилок; БУ - блок узгодження; БВП - блок виправлення помилок у кодовому слові.

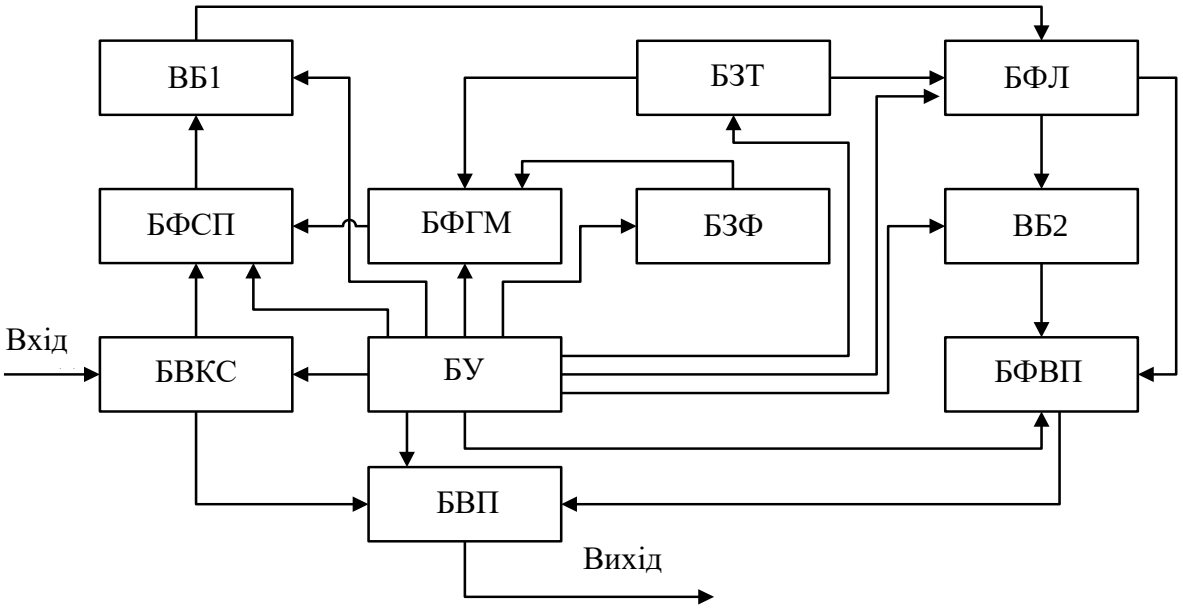


Рис. 3. Структурна схема пристрою декодування алгеброгеометричних кодів

Таким чином, у результаті проведених досліджень отримано загальне рішення задачі декодування алгеброгеометричних кодів побудованих за просторовими кривими, заданих у проективному просторі P^3 спільними рішеннями сукупності двох однорідних рівнянь від чотирьох змінних. Запропоновано алгебраїчний метод декодування алгеброгеометричних кодів по кривих у P^3, що дозволяє звести задачу декодування до розв'язання систем лінійних рівнянь, у яких число невідомих задається конструктивними кодовими характеристиками. Показано, що складність алгебраїчного декодування запропонованим методом росте поліноміально від виправляючої здатності коду.

У четвертому розділі обґрунтовується доцільність практичного використання алгеброгеометричних кодів на просторових кривих для підвищення завадостійкості передачі дискретних повідомлень і оцінка кодових співвідношень. Розглядається математична модель каналів передачі даних з незалежними помилками, досліджується методика оцінки завадостійкості. Досліджується завадостійкість передачі дискретних повідомлень у каналах з незалежними помилками при використанні алгеброгеометричних кодів на просторових кривих, обґрунтовуються практичні рекомендації їхнього використання.

Побудова ефективних завадостійких кодів у загальнотеоретичному плані пов'язано з побудовою довгих (з великим n) блокових кодів, що зберігають високі конструктивні кодові співвідношення (n, k, d). Аналіз кодових співвідношень алгеброгеометричних кодів показує, що при побудові через породжуючу матрицю (n, k, d) параметри зв'язані співвідношенням $(n \le N, k \ge \alpha - g + 1, d \ge n - \alpha)$, а при побудові через перевірочну матрицю - $(n \le N, k \ge n - \alpha + g - 1, d \ge \alpha - 2g + 2)$.

Таким чином, задачу побудови ефективних алгеброгеометричних кодів можна сформулювати таким чином: знайти регулярні методи побудови лінійних систем, що виникають на алгебраїчних кривих з великою кількістю точок N, стосовно роду кривої g.

Позначимо через w – розмірність простору P^w, над яким визначена крива X, через $N(X_w)$ і $g(X_w)$ – відповідну кількість точок і рід кривої X. Тоді загальним

критерієм вибору алгебраїчних кривих для побудови ефективних алгеброгеометричних кодів є вираз: $\lim_{w\to\infty}\left(N(X_w)/g(X_w)\right)>0$.На сьогоднішній день для просторових кривих відома узагальнена конструкція Артін-Шраєра (tower Artin-Schraier) над кінцевим полем $GF(p^2)$, що задається наступним виразом:

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

Для цієї просторової кривої відома оцінка кількості точок

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

і значення роду кривої:

$$g(X_w)=\begin{cases}p^w+p^{w-1}-p^{\frac{w+1}{2}}-2p^{\frac{w-1}{2}}+1, \textit{якщо } w-\textit{непарне;}\\ p^w+p^{w-1}-\frac{1}{2}p^{\frac{w+2}{2}}-\frac{3}{2}p^{\frac{w}{2}}-p^{\frac{w-2}{2}}+1, \textit{якщо } w-\textit{парне.}\end{cases}$$

У відомих роботах показано, що дана конструкція кривої досягає теоретичної границі Дрінфельда-Вледуца: $\lim_{g\to\infty}\left(N_q(g)/g\right)\leq\sqrt{q}-1$, яка встановлює граничне значення відношення числа раціональних точок кривої над кінцевим полем $GF(q)$ роду g. Таким чином, узагальнена конструкція Артін-Шраєра може розглядатися як реальне джерело кривих, для побудови ефективних завадостійких кодів.

На рис. 4 - 7 наведено залежності відносної швидкості кодування $R = k/n$ від відносної мінімальної кодової відстані $\delta = d/n$ для алгеброгеометричних кодів на просторових кривих Артін-Шраєра над $GF(p^2)$, p = 4, 8, 16, 32 - (1) та границя недвійкових БЧХ кодів тієї ж довжини - (2), а також, для порівняння, наведені верхня кодова границя Сінлгтона - (3) та нижня кодова границя Варшамова-Гілберта - (4).

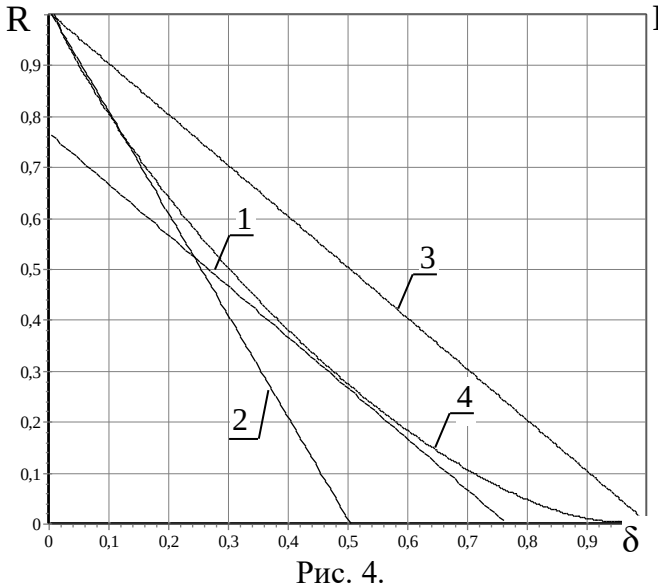


Рис. 4.

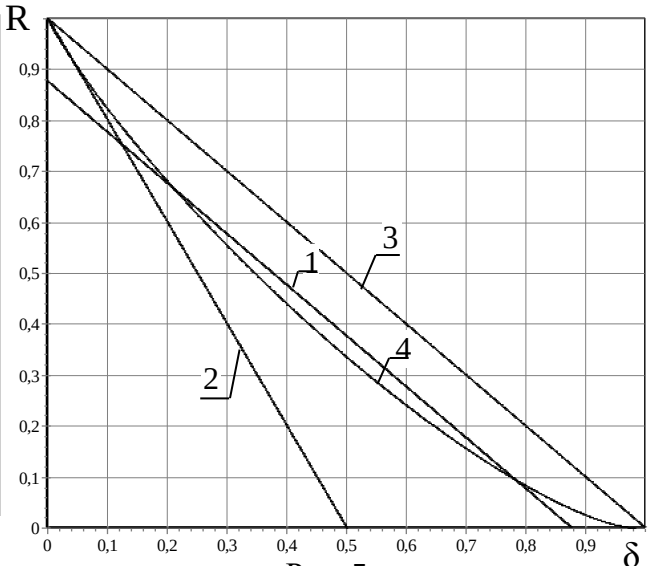
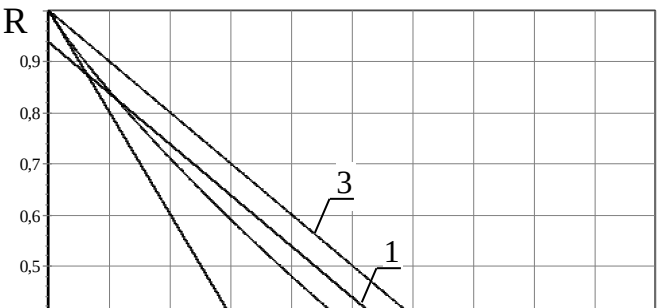
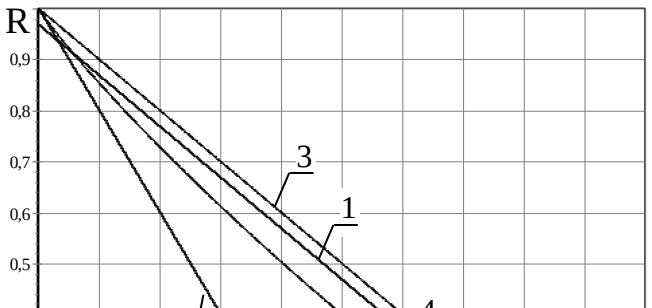


Рис. 5.

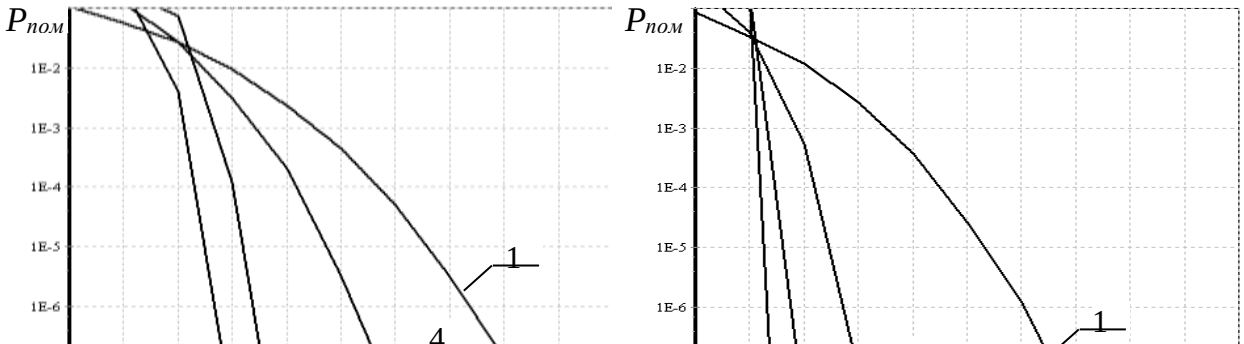




Таким чином, проведені дослідження показують, що алгеброгеометричні коди на просторових кривих Артін-Шраєра мають кодові співвідношення, які при збільшенні довжини коду й потужності алфавіту символів прагнуть до верхніх теоретичних границь (границі Сінлгтона).

Розглянемо процес передачі 16-овими символами при когерентному прийомі 16-ових ортогональних сигналів. На рис. 8 наведено залежності ймовірності помилки на один символ від співвідношення енергії сигналу до спектральної щільності потужності шуму, що приходиться на один біт: 1 – без кодування (когерентний прийом 16-ових ортогональних сигналів); 2 – з використанням алгеброгеометричного (240, 156, 65) коду на просторових кривих Артін-Шраєра над *GF(16)*; 3 – з використанням (240, 156, 47) коду БЧХ над *GF(16)*; 4 – з використанням (17, 11, 7) коду РС над *GF(16)*. Як показує аналіз наведених залежностей застосування (240, 156, 65) коду дозволяє отримати енергетичний виграш від кодування (ЕВК) 0,5 - 0, 8 дБ, що обумовлює відповідне підвищення завадостійкості передачі дискретних повідомлень.

Розглянемо процес передачі 64-ічними символами при когерентному прийомі 64-ічних ортогональних сигналів. На рис. 9 наведено залежності ймовірності помилки на один символ від співвідношення енергії сигналу до спектральної щільності потужності шуму, що приходиться на один біт: 1 – без кодування (когерентний прийом 64-ічних ортогональних сигналів); 2 – з використанням алгеброгеометричного (4032, 2667, 869) коду на просторових кривих Артін-Шраєра над *GF(64)*; 3 – з використанням (4032, 2667, 755) коду БЧХ над *GF(64)*; 4 – з використанням
(65, 45, 21) коду РС над *GF(64)*. Як показує аналіз наведених залежностей застосування (4032, 2667, 869) коду дозволяє отримати ЕВК 0,3 - 0,5 дБ, що обумовлює відповідне підвищення завадостійкості передачі дискретних повідомлень. Крім того, очевидно, що подальше збільшення довжини й потужності алфавіту символів приведе до подальшого росту ЕВК і наближення до границі Шеннона ймовірності помилкового прийому.



Таким чином, проведені дослідження показали, що застосування алгеброгеометричних кодів на просторових кривих дозволяє істотно підвищити завадостійкість передачі дискретних повідомлень у каналах з незалежними помилками.

Асимптотичні властивості алгеброгеометричних кодів при збільшенні довжини коду й потужності алфавіту символів обумовлюють наближення до Шенонівської границі ймовірності помилкового прийому символів повідомлення. Аналіз отриманих експериментальних результатів дозволяє зробити висновок про їх збіжність із теоретичними оцінками, що підтверджує вірогідність отриманих результатів.

У додатках наведено приклади побудови й декодування кодів на просторових кривих, опис і лістинг програмної реалізації алгоритмів побудови й декодування кодів на просторових кривих.

ВИСНОВКИ

У дисертаційній роботі отримано теоретичне узагальнення й нове вирішення важливої науково-технічного завдання, що полягає в розробці методів і алгоритмів побудови лінійних блокових кодів з покращеними властивостями для підвищення завадостійкості передачі дискретних повідомлень.

1. Найбільш ефективним засобом підвищення завадостійкості передачі дискретних повідомлень є методи канального (завадостійкого) кодування. Перспективним напрямком у їхньому розвитку є алгеброгеометричні коди на просторових кривих. Практичне використання таких кодів дозволить підвищити енергетичну ефективність передачі повідомлень каналами з випадковими помилками, що при фіксованій імовірності помилкового прийому символу повідомлення дозволяє підвищити завадостійкість передачі дискретних повідомлень.

2. При проведенні дисертаційних досліджень одержано нові кодові конструкції завадостійких кодів як лінійних систем, що виникають на просторових кривих, які відрізняються від відомих тим, що при фіксованій потужності алфавіту символів та без погіршення кодових співвідношень вдається побудувати лінійні блокові коди більшої довжини. Розроблено метод кодування алгеброгеометричними кодами на

просторових кривих, що відрізняється від відомих формуванням базису лінійного коду через відображення множини спільних рішень двох однорідних алгебраїчних рівнянь від чотирьох змінних, що дозволяє при фіксованій потужності алфавіту символів і при збереженні високих конструктивних кодових характеристик отримати більшу довжину коду. Розроблено алгебраїчний метод декодування алгеброгеометричних кодів на просторових кривих, що відрізняється від відомих формуванням триваріантного рівняння локаторів помилок, рішення якого однозначно задаються помилками, що відбулися, що дозволяє звести задачу декодування до розв'язання системи лінійних рівнянь, у яких число невідомих визначається конструктивними кодовими характеристиками.

3. Розроблено алгоритми й структурні схеми пристроїв завадостійкого кодування алгеброгеометричними кодами на просторових кривих. Показано, що формування кодових слів реалізується з використанням елементарних арифметичних операцій над елементами кінцевого поля й може бути виконано алгоритмами поліноміальної складності від параметрів коду. Формально, асимптотична ємкісна складність кодування *(n, k, d)* кодами оцінюється як *O(n)*, асимптотична часова складність оцінюється як *O(kn)* і *O((n-k)n)*. Розроблено алгоритми й структурні схеми пристроїв алгебраїчного декодування алгеброгеометричними кодами на просторових кривих. Показано, що складність алгебраїчного декодування запропонованим методом росте поліноміально від виправляючої здатності коду. Обґрунтовано доцільність реалізації розроблених декодерів на сучасній обчислювальній техніці при виправляючій здатності коду $t \leq 100$. Досліджено завадостійкість передачі дискретних повідомлень із використанням алгеброгеометричних кодів на просторових кривих. Показано, що при фіксованій потужності алфавіту символів і довжині застосування алгеброгеометричних кодів на просторових кривих дозволяє отримати енергетичний виграш від кодування *0,5-0,8 дБ* порівняно з недвійковими кодами БЧХ.

4. Результати дисертаційної роботи рекомендується використовувати при проведенні науково-дослідних і дослідно-конструкторських робіт зі створення нових засобів захисту інформації для підвищення завадостійкості передачі дискретних повідомлень каналами з випадковими помилками. Результати досліджень будуть корисні для підготовки фахівців у вищих навчальних закладах України при вивченні навчальних дисциплін з теорії інформації та завадостійкого кодування.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. *Пасько И.В.* Алгебраическое декодирование кодов на пространственных кривых. // Системи обробки інформації: Збірник наукових праць.– Х.: ХУ ПС, 2007. – Вип. 1 (59). – С. 121 - 125.

2. *Грабчак В.И. Пасько И.В. Лахтин С.Є. Королев Р.В.* Анализ математической модели и структурной схемы системы передачи данных // Системи обробки інформації: Збірник наукових праць. – Х.: ХУ ПС, 2007. – Вип. 4 (62). – С. 30 - 34.

3. *Грабчак В.И., Пасько И.В., Королев Р.В., Кужель И.Е*. Алгебраический метод помехоустойчивого кодирования алгеброгеометрическими кодами на

пространственных кривых // Системи управління, навігації та зв'язку. –К.: ЦНДІ навігації та управління, 2007. – Вип.3. – С. 82 - 85.

4. *Кузнецов А.А., Грабчак В.И., Пасько И.В.* Исследование помехоустойчивости передачи дискретных сообщений с использованием алгеброгеометрических кодов на пространственных кривых // Системи обробки інформації: Збірник наукових праць. –Х.: ХУПС, 2007. – Вип. 8 (66). – С. 134 - 138.

5. *Кузнецов О.О., Пасько І.В.* Алгебраїчний метод декодування лінійних блокових кодів на алгебраїчних кривих у P^3. // Системи озброєння і військова техніка: науковий журнал. – 2006. – № 3 (7). – С. 69 - 72.

6. *Кузнецов О.О., Пасько И.В., Королев Р.В.* Алгебраический метод помехоустойчивого кодирования алгеброгеометрическими кодами на пространственных кривых // Системи обробки інформації: Збірник наукових праць. –Х.: ХУПС, 2007. – Вип. 5 (63). – С. 137 - 141.

7. *Кузнецов А.А., Пасько И.В.* Алгоритм алгебраического декодирования линейных блоковых кодов на пространственных кривых // Тези доповідей Міжн. НТК "Інтегровані комп'ютерні технології в машинобудуванні" (ІКТМ-2006). – Х.: Нац. аерокосм. ун-т "ХАІ ", 2006. – С. 347.

8. *Кузнецов А.А., Пасько И.В.* Алгебраический метод декодирования линейных блоковых кодов на алгебраических кривых в P^3 // Тезисы докладов третьей международной научной конференции "Современные методы кодирования в электронных системах" СМКЭС-2006, 24-25 октября 2006 года. – Сумы: СумДУ, 2006. – С. 10-11.

9. *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».– Х.: НДІ макрографії, 2007 – С. 8-9.

10. *Пасько И.В.* Алгебраическое декодирование кодов на пространственных кривых // Матеріали третьої наукової конференції Харківського університету Повітряних Сил ім. Івана Кожедуба. – Х.:ХУПС, 2007. – С. 96-97.

АНОТАЦІЇ

Пасько І.В. Методи побудови лінійних блокових кодів з покращеними властивостями для підвищення завадостійкості передачі дискретних повідомлень. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за фахом 05.12.02 - телекомунікаційні системи і мережі. - Українська державна академія залізничного транспорту, Харків, 2008.

Дисертація присвячена вирішенню актуального науково-технічного завдання, що полягає в розробці методів і алгоритмів побудови лінійних блокових кодів з покращеними властивостями для підвищення завадостійкості передачі дискретних повідомлень. У ході проведених досліджень розроблено метод, алгоритми та

структурні схеми кодування і декодування алгеброгеометричними кодами на просторових кривих.

Показано, що формування кодових слів реалізується з використанням елементарних арифметичних операцій над елементами кінцевого поля і може бути виконано алгоритмами поліноміальної складності від параметрів коду. Складність алгебраїчного декодування запропонованим методом росте поліноміально від виправляючої здатності коду. Дослідження завадостійкості передачі дискретних повідомлень показали, що при фіксованій потужності алфавіту символів і довжині застосування алгеброгеометричних кодів на просторових кривих дозволяє отримати енергетичний виграш від кодування *0,5-0,8 дБ* порівняно з недвійковими кодами БЧХ.

Ключові слова: завадостійке кодування, передача дискретних повідомлень, алгебраїчний блоковий код.

Пасько И.В. Методы построения линейных блоковых кодов с улучшенными свойствами для повышения помехоустойчивости передачи дискретных сообщений. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.12.02 – телекоммуникационные системы и сети. – Украинская государственная академия железнодорожного транспорта, Харьков, 2008.

Диссертация посвящена решению актуальной научно-технической задачи, состоящей в разработке методов и алгоритмов построения линейных блоковых кодов с улучшенными свойствами для повышения помехоустойчивости передачи дискретных сообщений.

В данной работе показано, что эффективным средством повышения помехоустойчивости передачи дискретных сообщений являются методы канального (помехоустойчивого) кодирования. Перспективным направлением в их развитии являются алгеброгеометрические коды на пространственных кривых. Практическое использование таких кодов позволит повысить энергетическую эффективность передачи сообщений по каналам со случайными ошибками, что при фиксированной вероятности ошибочного приема символа сообщения позволяет повысить помехоустойчивость передачи дискретных сообщений.

В ходе проведенных исследований получены новые кодовые конструкции помехоустойчивых кодов как линейных систем возникающих на пространственных кривых, отличающиеся от известных тем, что при фиксированной мощности алфавита и без ухудшения кодовых соотношений удается построить линейные блоковые коды большей длины.

Разработан метод кодирования алгеброгеометрическими кодами на пространственных кривых, отличающийся от известных формированием базиса линейного кода через отображение множества совместных решений двух однородных алгебраических уравнений от четырех переменных, что позволяет при фиксированной мощности алфавита символов и при сохранении высоких конструктивных кодовых характеристик получить бóльшую длину кода. Предложенный метод развивает отдельное направление теории помехоустойчивого

кодирования и является дальнейшим развитием известных методов кодирования кодами на кривых, заданными в проективном пространстве P^2 решениями однородного уравнений от трех переменных (кодами на плоских кривых).

Получено общее решение задачи декодирования алгеброгеометрических кодов построенных по пространственным кривым, заданных в проективном пространстве P^3 совместными решениями совокупности двух однородных уравнений от четырех переменных.

Разработан алгебраический метод декодирования алгеброгеометрических кодов на пространственных кривых, который отличается от известных формированием трехвариантного уравнения локаторов ошибок, решения которого однозначно задаются произошедшими ошибками, что позволяет свести задачу декодирования к решению системы линейных уравнений, у которых число неизвестных определяется конструктивными кодовыми характеристиками.

Разработаны алгоритмы и структурные схемы устройств помехоустойчивого кодирования алгеброгеометрическими кодами на пространственных кривых. Показано, что формирование кодовых слов реализуется с использованием элементарных арифметических операций над элементами конечного поля и может быть выполнено алгоритмами полиномиальной сложности от параметров кода. Формально, асимптотическая емкостная сложность кодирования (n, k, d) кодами оценивается как $O(n)$, асимптотическая временная сложность оценивается как $O(kn)$ и $O((n-k)n)$.

Разработаны алгоритмы и структурные схемы устройств алгебраического декодирования алгеброгеометрическими кодами на пространственных кривых. Показано, что сложность алгебраического декодирования предложенным методом растет полиномиально от исправляющей способности кода. Обоснована целесообразность реализации разработанных декодеров на современной вычислительной технике при исправляющей способности кода $t \leq 100$.

Исследована помехоустойчивость передачи дискретных сообщений с использованием алгеброгеометрических кодов на пространственных кривых. Обоснован выбор обобщенной конструкции Артин-Шраера как реального источника кривых, для построения эффективных помехоустойчивых кодов. Получены оценки кодовых соотношений алгеброгеометрических кодов, построенных на пространственных кривых Артин-Шраера. Показано, что при фиксированной мощности алфавита символов и длине применение алгеброгеометрических кодов на пространственных кривых позволяет получить энергетический выигрыш от кодирования *0,5-0,8 dB* по сравнению с недвоичными кодами БЧХ.

Ключевые слова: помехоустойчивое кодирование, передача дискретных сообщений, алгебраический блоковый код.

Pasko I.V. Methods of linear sectional codes' construction with improved properties for the increasing of discrete messages antijamming passing. Typescript.

Dissertation on the receipt of scientific degree of candidate of technical sciences on speciality 05.12.02 – telecommunication systems and networks. –Ukrainian state academy of railway transport, Kharkiv, 2007.

Dissertation is devoted the decision of urgent scientific and technical task which consists in development of methods and algorithms of construction of linear sectional codes with improved properties for the increasing of discrete messages antijamming passing. During the conducted researches a method, algorithms and flow diagrams of code and decoding algebrogeometrical codes on spatial curves are developed

It is demonstrated that forming of code words will be realized with the use of elementary arithmetic operations above the elements of the eventual field and it can be executed the algorithms of polynomial complication from the parameters of code. Complication of algebra' decoding the offered method grows polynomial from correcting code capability. Discrete messages antijamming passing researches demonstrated that at the fixed alphabet' power of characters and length of algebrogeometrical codes on spatial curves application allowed to get the power winning from a code *0, 5-0,8 d* in comparing to the unbinary codes of BCH.

Keywords: antijamming code, discrete messages passing, algebraical sectional code .