УДК 621.391

ОЦІНКА ЕНЕРГЕТИЧНОЇ ЕФЕКТИВНОСТІ АЛГЕБРОГЕОМЕТРИЧНИХ КОДІВ НА ПРОСТОРОВИХ КРИВИХ

І.В. Пасько, *канд. техн. наук;*
О.М. Авдєєва

Науковий центр БЗ РВ і А Сумського державного університету, м. Суми

Исследуется энергетическая эффективность передачи дискретных сообщений М-ми ортогональными сигналами с использованием алгеброгеометрических кодов на пространственных кривых. Дается оценка энергетическому преимуществу алгеброгеометрического кодирования.

Досліджується енергетична ефективність передачі дискретних повідомлень М-ми ортогональними сигналами при застосуванні алгеброгеометричних кодів на просторових кривих. Оцінюється енергетичний виграш алгеброгеометричного кодування.

ВСТУП

Важливим показником ефективності сучасних телекомунікаційних систем і мереж є завадостійкість передачі дискретних повідомлень. Вона характеризує здатність системи забезпечити передачу дискретних повідомлень із заданою імовірністю помилки в умовах впливу перешкод усіх видів [1]. Найбільш ефективними засобами підвищення завадостійкості передачі дискретних повідомлень є методи завадостійкого кодування. Основними вимогами до завадостійкого кодування є висока здатність коду щодо виявлення та виправлення помилок, низька внесена надлишковість, висока швидкодія та низька складність реалізації процедур кодування-декодування. Головним завданням завадостійкості кодування інформації є підвищення енергетичної ефективності телекомунікаційних систем.

Недвійкові алгебраїчні блокові коди, асоційовані з алгебраїчними кривими (алгеброгеометричні коди), мають високу виправну здатність при невеликій частці внесеної надлишковості [2]. Асимптотично алгеброгеометричні коди на просторових кривих за своїми параметрами перебувають вище нижньої кодової границі Варшамова-Гілберта [3-5]. Їх практичне використання дозволяє підвищити енергетичну ефективність передачі дискретних повідомлень, що при фіксованій імовірності помилкового прийому символів повідомлення суттєво знижує вимоги до мінімально необхідного співвідношення енергії сигналу до спектральної густини потужності шуму [6].

У статті досліджується завадостійкість передачі дискретних повідомлень у каналах із незалежними помилками при використанні алгеброгеометричних кодів на просторових кривих, проводиться оцінка енергетичного виграшу алгеброгеометричних кодів на просторових кривих, порівняння потенційної завадостійкості М-х ортогональних сигналів і тієї завадостійкості, яка досягається при використанні алгеброгеометричних кодів, що задані на просторових кривих.

РОЗРАХУНОК ПОТЕНЦІЙНОЇ ЗАВАДОЗАХИЩЕНОСТІ М-х ОРТОГОНАЛЬНИХ СИГНАЛІВ

Під час некодованої передачі повідомлень імовірність помилкового прийому М-х символів при когерентному прийомі ортогональних сигналів визначається виразом [6]:

$$P_o = 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{u^2}{2}} \left[\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{u+\sqrt{2\gamma}} e^{-\frac{z^2}{2}} dz \right]^{M-1} du\ , \qquad (1)$$

де γ - відношення енергії сигналу до спектральної густини потужності шуму для М-го сигналу, $M = 2^{\mathrm{m}}$;

γ_{bit} - нормоване відношення енергії сигналу до спектральної густини потужності шуму на двійкову одиницю, $\gamma_{\mathrm{bit}} = \gamma / m$.

На рис.1 наведені залежності імовірності помилкового прийму М-го символу при когерентному прийомі ортогональних сигналів[7].

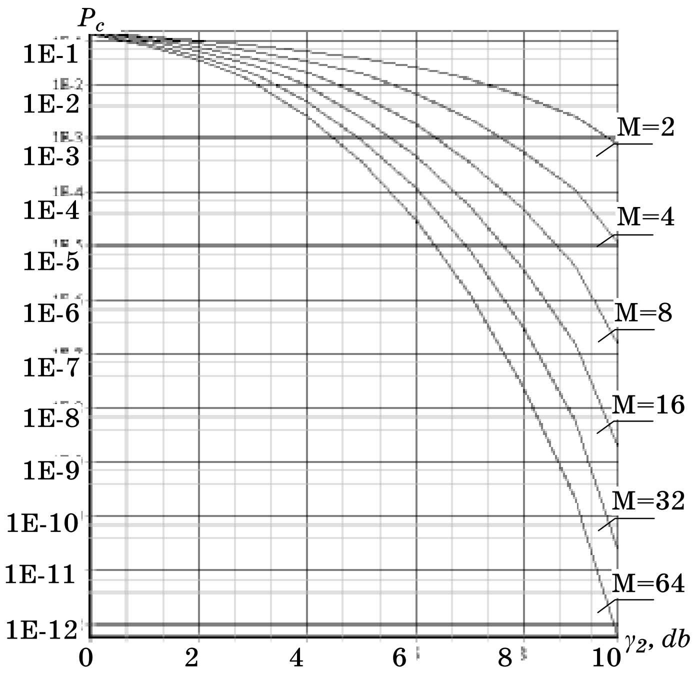

Рисунок 1–- Залежності імовірності помилкового прийому М-х символів від нормованого енергетичного відношення сигнал/шум, що припадає на один біт

Передача М-х ортогональних сигналів дозволяє отримати значний виграш завадостійкості при фіксованому співвідношенні сигнал/шум або суттєвий енергетичний виграш при фіксованій імовірності помилки символу. При збільшенні потужності ансамблю сигналів цей виграш зростає.

Метою даної роботи є оцінка енергетичної ефективності алгеброгеометричних кодів, що задані на просторових кривих.

АЛГЕБРОГЕОМЕТРИЧНЕ КОДУВАННЯ ІНФОРМАЦІЇ

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

$$\begin{cases} f_1\left(x_0, x_1, x_2, x_3\right) = 0, \\ f_2\left(x_0, x_1, x_2, x_3\right) = 0. \end{cases} \tag{2}$$

Нехай $p_0\left(x_0, x_1, x_2, x_3\right)$, $p_1\left(x_0, x_1, x_2, x_3\right)$, ..., $p_{N-1}\left(x_0, x_1, x_2, x_3\right)$ – N сумісних розв'язків системи рівнянь (1) – точок просторової кривої X.

Зафіксуємо дивізор D кривої X і множину раціональних функцій, асоційованих із дивізором D, тобто множину, яка складається із нуля і функції $f \neq 0$, для яких $\left(f\right) + D \geq 0$. Це еквівалентно набору генераторних функцій

$$F_0\left(x_0, x_1, x_2, x_3\right),\ F_1\left(x_0, x_1, x_2, x_3\right),\ F_2\left(x_0, x_1, x_2, x_3\right),\ ...,\ F_m\left(x_0, x_1, x_2, x_3\right),$$

де $F_0, F_1, ..., F_m$ - форми однакового ступіня і $F_0(x_0, x_1, x_2, x_3) \neq 0$.

Інакше кажучи, $j(x) = \left(F_0(x), F_1(x), ..., F_m(x)\right)$, як точка в P^m.

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

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

Загальним критерієм вибору алгебраїчних кривих для побудови ефективних алгеброгеометричних кодів є вираз [8]:

$$\lim_{w \circledR \Gamma} \frac{N(X_w)}{g(X_w)} > 0.$$

Для просторових кривих відома узагальнена конструкція Артін-Шраєра над кінцевим полем $GF(\mathrm{p}^2)$, яка задана таким виразом [8]:

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

Для цієї просторової кривої відома оцінка кількості точок

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

та значення роду кривої

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

Використовуючи конструкцію Артін-Шраєра для випадку $w = 3$ (випадок просторових кривих у P^3). Отримаємо просторову криву, що задана сукупністю рішень двох однорідних алгебраїчних рівнянь від 4 змінних над $\mathrm{GF}(p^2)$:

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

Род кривої та кількість точок над $\mathrm{GF}(p^2)$ задовольняє вираз

$$g = p^3 - 2p + 1,$$

$$N \geq p^4 - p^2.$$

Відношення кількості точок до роду кривої запишемо у вигляді виразу

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

У таблиці 1 наведені експериментальні оцінки кодових співвідношень алгеброгеометричних кодів на просторових кривих Артін-Шраєра над GF(4) і GF(16).

Таблиця 1 – Експериментальна оцінка кодових відношень алгеброгеометричних кодів на просторових кривих Артін-Шраєра

deg F	*k*	*d*	$k_\perp$	$d_\perp$
g=5, *n*=12 над *GF* (4);				
1	4	6	8	2
2	10	2	2	8
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

Проведемо оцінку енергетичного виграшу алгеброгеометричних кодів, що пропонуються.

МАТЕМАТИЧНА МОДЕЛЬ КАНАЛУ ПЕРЕДАЧІ ДАНИХ І ОЦІНКА ЗАВАДОСТІЙКОСТІ ПЕРЕДАЧІ ДИСКРЕТНИХ ПОВІДОМЛЕНЬ

Нехай задано код (n,k,d). Припустимо, що під час передачі кодового слова помилки виникають незалежно з імовірністю P_o. Тоді імовірність помилки кратності i на довжині блоку n становить

$$P\left(i,n\right) = C_{\mathrm{n}}^{\mathrm{i}} P_{\mathrm{o}}^{\mathrm{i}} \left(1 - P_o\right)^{n-i}. \tag{3}$$

Імовірність спотворення кодової комбінації $\geq$ m помилками запишеться у вигляді

$$P(\geq m,n)=\sum_{\mathrm{i=m}}^{\mathrm{n}}P(i,n).$$

Для моделі з незалежними помилками значення $P(\geq m,n)$ визначається як

$$P(\geq m,n)=\sum_{i=m}^{n}C_n^i P_o^i\left(1-P_{\mathrm{o}}\right)^{n-i}. \tag{4}$$

Якщо декодер виправляє $t=(d-1)/2$ помилок, то імовірність помилкового декодування блоку

$$P_{\text{од}}(n)=1-\sum_{\mathrm{i=0}}^{\mathrm{t}}C_n^i P_o^i\left(1-P_{\mathrm{o}}\right)^{n-i}-\sum_{\mathrm{i=t+1}}^{\mathrm{n}}u(i)P_o^i\left(1-P_{\mathrm{o}}\right)^{n-i}, \tag{5}$$

де $C_{\mathrm{n}}^{\mathrm{i}}$ – біноміальний коефіцієнт; $u(i)$ – число векторів помилок ваги i, які виправляють код.

Якщо код виправляє всі помилки у межах радіуса упаковки коду і не виправляє інші помилки, то

$$P_{\text{од}}(n)=P(>t,n)=\sum_{i=t+1}^{n}C_n^i P_o^i\left(1-P_o\right)^{n-i}. \tag{6}$$

Для перерахунку імовірності помилки декодування на один символ $P_{\text{пом}}$ скористаємося виразом

$$P_{\text{пом}}=\frac{d}{n}P_{\text{од}}(n)=\frac{d}{n}\sum_{i=t+1}^{n}C_n^i P_o^i\left(1-P_o\right)^{n-i}. \tag{7}$$

Застосування (n, k, d) блокових кодів над $GF(2^{\mathrm{m}})$, які виявляють та виправляють помилки, призводить до збільшення надлишкових даних, що передаються. Якщо зафіксувати енергію повідомлення, яке передається в канал, то енергія, що припадає на один символ, зменшиться пропорційно до внесеної надлишковості. Для розрахунку імовірності помилки на символ на виході декодера за виразом (7) із урахуванням внесеної надлишковості відношення енергії сигналу до спектральної густини потужності шуму γ у виразі (1) зменшиться у n/k раз.

Для оцінки завадостійкості передачі дискретних повідомлень розглянемо процес передачі 16-ми символами при когерентному прийомі 16-х ортогональних сигналів. На рис. 2 наведено залежності ймовірності помилки на один символ від співвідношення енергії сигналу до спектральної густини потужності шуму, що припадає на один біт: 1 – без кодування (когерентний прийом 16-х 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-ми символами при когерентному прийомі 64-х ортогональних сигналів. На рис. 3 наведено залежності ймовірності помилки на один символ від співвідношення енергії сигналу до спектральної густини потужності шуму, що припадає на один біт: 1 – без кодування (когерентний прийом 64-х 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).

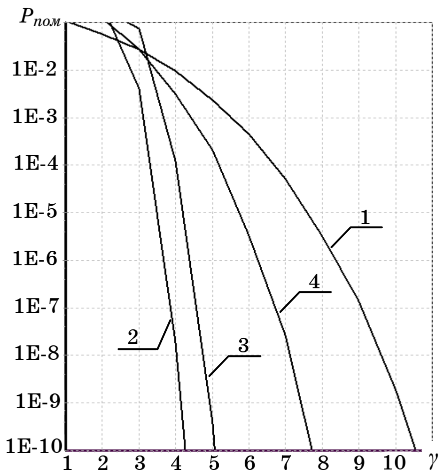

Рисунок 2 – Залежності імовірності помилки 16-х символів від співвідношення енергії сигналу до спектральної густини потужності шуму

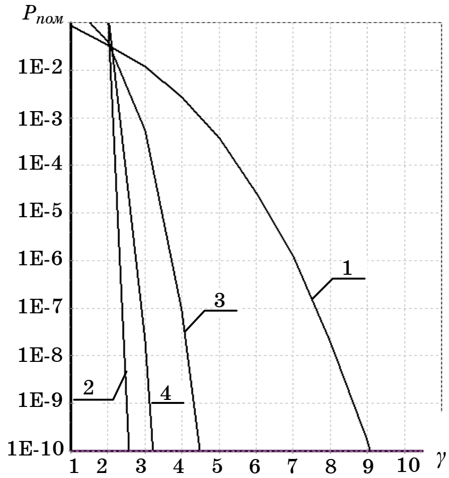

Рисунок 3–- Залежності імовірності помилки 64-х символів від співвідношення енергії сигналу до спектральної густини потужності шуму

Як показує аналіз наведених залежностей, застосування алгеброгеометричних кодів на просторових кривих 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 зростання ЕВК і наближення до границі Шеннона імовірності помилкового прийому.

ВИСНОВКИ

Таким чином, проведені дослідження показали, що 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. 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.

SUMMARY

EVALUATION OF POWER EFFICIENCY OF ALGEBROGEOMETRICAL CODES ON SPACE CURVES

__I.V. Pasko, J.M. Avdeyeva__
Sumy State University

Power efficiency of transmission of discrete messages by orthogonal M-signals under using algebrogeometrical codes on space curves is investigated. Power gain of algebrogeometrical encoding is evaluated.

СПИСОК ЛІТЕРАТУРИ

1. Влэдуц С. Г., Манин Ю. И. Линейные коды и модулярные кривые //Современные проблемы математики. – 1984. - Т. 25. - С. 209-257.
2. Гоппа В.Д. Коды и информация // Успехи математических наук. – 1984. – Т.30, Вып. 1(235). – С. 77-120.
3. Цфасман М.А. Коды Гоппы, лежащие выше границы Варшамова-Гилберта // Проблемы передачи информации. – 1982. – Т.18, №3. – С. 3-6.
4. Гоппа В.Д. Коды на алгебраических кривых //Докл. АН СССР. – 1981. – Т.259. № 6. – С. 1289-1290.
5. Влэдуц С. Г., Ногин Д.Ю., Цфасман М.А. Алгеброгеометрические коды. Основные понятия. – М.: МЦИМО, 2003. – 504 с.
6. 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. – Харків: ХУПС, 2007. – Вип. 8 (66). – С. 134 - 138.
7. Кузнецов А.А. Методика оценки эффективности помехоустойчивого кодирования в каналах с группирующимися ошибками // Электронное моделирование: Международный научно-теоретический журнал. – 2006.–№3.– С. 49-60.
8. Ляпа Н.Н., Грабчак В.И., Пасько И.В. Исследование алгеброгеометрических кодов на пространственных кривых Артин-Шраера для повышения помехоустойчивости передачи дискретных сообщений // Вісник Сумського державного університету. Технічні науки. - 2007. - №2 – С. 140-147.

Надійшла до редакції 24 березня 2009 р.