УДК 621.391

М.І. Науменко, Ю.В. Стасєв, О.О. Кузнецов

АЛГЕБРОГЕОМЕТРИЧНЕ УЗАГАЛЬНЕННЯ ЛІНІЙНИХ БЛОКОВИХ КОДІВ

Досліджується основна проблема теорії завадостійкого кодування: побудова кодів з великою відносною швидкістю та з великою мінімальною кодовою відстанню. Запропоновано теоретичне узагальнення найбільш важливих класів алгебраїчних блокових кодів через обмеження алгеброгеометричних кодів на довільному підполі.

Постановка проблеми в загальному вигляді та аналіз літератури

Важливим показником ефективності систем керування військами і зброєю є вірогідність військового зв'язку, яка виражається у здатності забезпечувати точне відтворення переданих повідомлень у пунктах приймання. Показником оцінки вірогідності є імовірність правильного приймання ($P_{пп}$). Як зворотна величина також використовується показник утрати вірогідності – імовірність хибного приймання повідомлення ($P_{пом} = 1 - P_{пп}$).

Сучасні вимоги з вірогідності переданих даних в АСУВ істотно зросли. Так, відповідно до системи загальних технічних вимог до видів озброєнь і військової техніки, вимоги до перспективних комплексів автоматизації і зв'язку складають $P_{пом} < 10^{-9} - 10^{-12}$.

Одним з основних і найбільш ефективних засобів підвищення вірогідності переданих даних по каналах АСУВ є завадостійке кодування. Воно полягає у внесенні за визначеним алгоритмом у передані дані надлишковості (перевірочної частини). На приймальній стороні декодер аналізує відповідність переданих даних внесеній надмірності і зменшує дію помилок, що виникли при передаванні.

Основна проблема теорії завадостійкого кодування вперше сформульована в роботі Шеннона [1] – знайти коди з великою відносною швидкістю R і з великою мінімальною кодовою відстанню d. Вона випливає з наступної теореми.

Теорема 1 [1]. Нехай $C(P_0)$ – пропускна здатність дискретного симетричного каналу з імовірністю помилки P_0. Тоді для кожного $\varepsilon > 0$, якщо $R < C(P_0)$ і n досить велике, існує (n, k, d) код з відносною швидкістю $k / n \geq R$, імовірність помилки декодування якого $P_{ош} < \varepsilon$.

Теорема 1 доведена імовірнісними методами і не дає механізм для побудови хороших кодів. Найбільший розвиток у теорії кодування одержали лінійні блокові коди, для яких справедлива наступна теорема.

Теорема 2 [2]. Якщо виконується рівняння

$$q^{n-k} \geq \sum_{i=0}^{d-2} C_{n-1}^{i} (q-1)^{i}, \qquad (1)$$

то існує лінійний (n, k, d) код над GF(q).

Теорема 2 гарантує існування хороших лінійних кодів над GF(q) з параметрами (n, k, d), що задовольняють виразу (1), який одержав назву межі Варшамова-Гілберта. На практиці частіше використовують асимптотичні межі, що дають уявлення про граничні кодові характеристики при нескінченно великій довжині коду. Прологарифмуємо вираз (1) та одержимо

$$n - k \geq \log_q \left(\sum_{i=0}^{d-2} C_{n-1}^{i} (q-1)^{i} \right).$$

Якщо спрямуємо $n \to \infty$, одержимо асимптотичну межу Варшамова-Гілберта:

$$R \leq 1 - H_q(\delta), \qquad (2)$$

де $\delta = d / n$ – відносна мінімальна відстань коду як частка помилок у прийнятому слові, які може знайти код;

$H_q(x)$ – q-а функція ентропії на відрізку

$$\left[0, \frac{q-1}{q} \right],$$

причому

$$H_q(x) = x \log_q (q-1) - x \log_q (x) - (1-x) \log_q (1-x),$$

$$0 < x \leq \frac{q-1}{q}.$$

Таким чином, проблема завадостійкого кодування полягає в пошуку регулярних алгоритмів побудови таких лінійних блокових (n, k, d) кодів, параметри яких задовольняють кодову межу (1) і/або асимптотичні кодові межі яких задовольняють вираз (2).

Мета статті – виклад загальнотеоретичних положень алгебраїчної теорії блокових кодів, теоретичне узагальнення найбільш важливих класів алгебраїчних блокових кодів через обмеження лінійних

блокових кодів, що виникають на алгебраїчних кривих (алгеброгеометричних кодів) на довільне підполе, розробка методів і регулярних алгоритмів побудови алгеброгеометричних кодів, алгоритмів кодування і декодування.

Основний матеріал

1. Загальні положення алгебраїчної теорії блокових кодів. Першим успішним результатом побудови лінійних блокових кодів є циклічні коди [2 – 6].

Кожен лінійний (n, k, d) код над GF(q) є підпростором $GF^k(q)$ простору $GF^n(q)$. Циклічний код є поодиноким випадком підпростору, тому що має додаткову властивість циклічності. Кожен вектор з $GF^n(q)$ можна представити многочленом від формальної змінної x ступеня не вище n – 1. Компоненти вектора ототожнюються з коефіцієнтами многочлена. Множина многочленів має структуру векторного простору, яка ідентична структурі простору $GF^n(q)$, а також структуру кільця многочленів $GF(q)[x]/(x^n - 1)$. У кільці многочленів визначено множення

$$p_1(x) \cdot p_2(x) = R_{x^n-1}\left[p_1(x) \cdot p_2(x)\right],$$

тоді циклічний зсув запишеться у вигляді

$$x \cdot p(x) = R_{x^n-1}\left[x \cdot p(x)\right].$$

Якщо кодові слова (n, k, d) коду над GF(q) задаються у вигляді многочленів, то код є підмножиною кільця $GF(q)[x]/(x^n - 1)$. Код є циклічним, якщо разом з кодовим словом c(x) він містить також многочлен x c(x).

Справедлива наступна теорема.

Теорема 3 [2]. Єдиний наведений ненульовий многочлен g(x) найменшого степеня r = n – k однозначно задає (n, k, d) циклічний код над GF(q) і позначається породним многочленом, причому

$$g(x) = \prod_i (x - \beta^i),$$

де $\beta^i \in GF(q^m)$.

Многочлен g(x) ділить многочлен $x^n - 1$, який у свою чергу ділить многочлен $x^m - 1$, так що g(x) ділить також $x^{q^m-1} - 1$. Нехай α – примітивний елемент поля $GF(q^m)$, $q^m - 1 = n$ b і $\beta = \alpha^b$. Тоді всі корені многочлена $x^n - 1$, як і корені многочлена g(x), вичерпуються степенями елемента β. Прості дільники многочлена $x^n - 1$ мають своїми коренями тільки такі елементи. Іншими словами, якщо використовувати $\beta = \alpha^b$ замість α і обмежитися множиною породного многочлена у вигляді степенів β, то одержимо код довжини $n = (q^m - 1) / b$. Якщо b = 1, то $\beta = \alpha$, $n = q^m - 1$, такий код називають примітивним [2 – 4].

Якщо $g(x) = g_0 + g_1x + g_2x^2 + \ldots g_rx^r$, то в матричній формі циклічний код задається своєю породною матрицею

$$G = \begin{pmatrix} 0 & \ldots & g_{n-k} & g_{n-k-1} & \ldots & g_1 & g_0 \\ 0 & \ldots & g_{n-k-1} & \ldots & g_1 & g_0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ g_{n-k} & g_{n-k-1} & \ldots & \ldots & \ldots & 0 & 0 \end{pmatrix}$$

або перевірочною матрицею

$$H = \begin{pmatrix} 0 & 0 & \ldots & \ldots & \ldots & h_{k-1} & h_k \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & h_0 & h_1 & \ldots & h_k & 0 & 0 \\ h_0 & h_1 & \ldots & h_k & \ldots & 0 & 0 \end{pmatrix},$$

де $h(x) = h_0 + h_1x + h_2x^2 + \ldots h_kx^k$ – перевірочний многочлен циклічного коду, $h(x) \cdot g(x) = x^n - 1$.

Найбільше поширення серед циклічних кодів одержали коди Боуза-Чоудхурі-Хоквінхгема (БЧХ), у яких як корені g(x) використовується 2t послідовних степенів довільного елемента $\beta \in GF(q^m)$ (як показано вище, не обов'язково примітивного). Іншими словами породний многочлен визначається як

$$g(x) = \text{H.O.K. } [f_j(x), f_{j+1}(x), \ldots, f_{j+2t-1}(x)], \quad (3)$$

де $f_i(x)$ – мінімальний многочлен елемента $\beta^i \in \in GF(q^m)$, i = j, …, j + 2t – 1...

Коренями $f_i(x)$ є також всі елементи класу спряжених елементів

$$\left\{\beta^i, \left(\beta^i\right)^q, \left(\beta^i\right)^{q^2}, \ldots, \left(\beta^i\right)^{q^{s-1}}\right\},$$

де s – найменше ціле число, таке, що

$$\beta^{q^s} = \beta, \; s < m.$$

Довжина коду дорівнює порядкові елемента β, тобто найменшому n, для якого $\beta^n = 1$. Отже, код БЧХ можна задати перевірочною матрицею вигляду

$$H = \begin{pmatrix} \beta^0 & \beta^j & \beta^{2j} & \ldots & \beta^{(n-1)j} \\ \beta^0 & \beta^{j+1} & \beta^{j+2} & \ldots & \beta^{(n-1)(j+1)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \beta^0 & \beta^{j+2t-1} & \beta^{j+2t} & \ldots & \beta^{(n-1)(j+2t-1)} \end{pmatrix}, \quad (4)$$

де кожен елемент повинен бути замінений на відповідний стовпець з m елементів над GF(q).

Справедлива наступна теорема.

Теорема 4 [2]. Параметри циклічного блокового (n, k, d) коду БЧХ над GF(q), заданого породним многочленом вигляду (3) з коренями $\beta \in GF(q^m)$, задовольняють умові

$$d \geq 2t + 1, \; k \geq n - m\,2t.$$

Теорема 4 дає нижню межу розмірності коду

БЧХ і його мінімальної кодової відстані. Кодові параметри більшості кодів БЧХ як правило лежать вище цієї межі. Так, наприклад, над $GF(2^m)$ виконується рівність $f_j(x) = f_{2j}(x)$, отже, для примітивного двійкового коду БЧХ кодові межі з теореми 4 можна переписати у вигляді

$$d \ge 2t + 1,\ k \ge n - m \cdot t.$$

Породна матриця запишеться у вигляді

$$H = \begin{pmatrix} \beta^0 & \beta^1 & \beta^2 & \dots & \beta^{n-1} \\ \beta^0 & \beta^3 & \beta^6 & \dots & \beta^{3(n-1)} \\ \dots & \dots & \dots & \dots & \dots \\ \beta^0 & \beta^{2t-1} & \beta^{2t} & \dots & \beta^{(n-1)(2t-1)} \end{pmatrix},$$

де кожен елемент заміняються відповідним m-розрядним двійковим стовпцем. Короткі коди БЧХ володіють хорошими кодовими параметрами і лежать вище межі Варшамова-Гілберта. На жаль, із зростанням довжини коду їх характеристики погіршуються.

Розглянемо випадок для m = 1. Тоді поле символів (n, k, d) коду над GF(q) збігається з полем $GF(q^m)$. Якщо код примітивний, то одержимо код Ріда-Соломона (РС), довжина якого дорівнює $n = q^m - 1 = = q - 1$.

Справедлива наступна теорема.

Теорема 5 [2]. Код РС має мінімальну відстань d = n – k + 1 і є кодом з максимально досяжною кодовою відстанню (МДВ кодом). Породний многочлен запишеться у вигляді

$$g(x) = \prod_{i=j}^{j+2t-1} (x - \beta^i),$$

де t – конструктивна здатність коду, що виправляє $t = \lfloor (d-1)/2 \rfloor$, причому n – k = 2t. Породна матриця відповідає виразу (4).

Вираз

$$d \le n - k + 1$$

(границя Синлгтона) встановлює верхню межу для параметрів лінійного блокового (n, k, d) коду [2 – 4]. Теорема 4 стверджує, що при фіксованих n і k не існує коду, у якого мінімальна відстань більше, ніж у кода РС. Водночас коди РС є коротшими за всі інші циклічні коди над тим же алфавітом.

Визначення 1 [2, 4]. Нехай $X = (X_1, X_2, \dots, X_n)$ – вектор над $GF(q^m)$, причому всі X_i – різні елементи $GF(q^m)$. Нехай також $h = (h_1, h_2, \dots, h_n)$ – вектор над $GF(q^m)$ з необов'язково різними h_i елементами $GF(q^m)$. Тоді (n, k, d) узагальнений код Ріда-Соломона $OPC_k(X, h)$ складається з усіх векторів вигляду

$$(h_1 \cdot F(X_1), h_2 \cdot F(X_2), \dots, h_n \cdot F(X_n)),$$

де F(x) – будь-який многочлен з коефіцієнтами з $GF(q^m)$, степінь якого не перевищує k. Код ОРС є кодом з максимально досяжною кодовою відстанню, тобто d = r + 1, r = n – k. Перевірочна матриця $OPC_k(X, h)$ дорівнює

$$H = \begin{pmatrix} Y_1 & Y_2 & \dots & Y_n \\ X_1 \cdot Y_1 & X_2 \cdot Y_2 & \dots & X_n \cdot Y_n \\ X_1^2 \cdot Y_1 & X_2^2 \cdot Y_2 & \dots & X_n^2 \cdot Y_n \\ \dots & \dots & \dots & \dots \\ X_1^{r-1} \cdot Y_1 & X_2^{r-1} \cdot Y_2 & \dots & X_1^{r-1} \cdot Y_n \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 1 & \dots & 1 \\ X_1 & X_2 & \dots & X_n \\ X_1^2 & X_2^2 & \dots & X_n^2 \\ \dots & \dots & \dots & \dots \\ X_1^{r-1} & X_2^{r-1} & \dots & X_1^{r-1} \end{pmatrix} \cdot \begin{pmatrix} Y_1 & 0 & \dots & 0 \\ 0 & Y_2 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & Y_n \end{pmatrix}, \quad (5)$$

де вектор $Y = (Y_1, Y_2, \dots, Y_n)$ такий, що $\forall Y_i \in GF(q^m)$, $Y_i \ne 0$ і $OPC^{\perp}_k(X, h) = OPC_r(X, Y)$.

Коди ОРС дають механізм побудови великого класу альтернантних кодів [2].

Визначення 2 [2, 4]. Альтернантний (n, k, d) код A(X, h) складається з усіх слів коду $OPC^{\perp}_k(X, h)$ таких, що їх компоненти лежать у полі GF(q). Іншими словами, A(X, h) дорівнює обмеженню коду $OPC_k(X, h)$ на підполі GF(q). Таким чином, A(X, h) складається з усіх векторів X над GF(q), що задовольняють рівність

$$H X^T = 0,$$

де H – перевірочна матриця $OPC_k(X, h)$, що задається виразом (5).

Параметри альтернантного (n, k, d) коду A(X, h) пов'язані співвідношенням

$$n - mr \le k \le n - r;\ d \ge r + 1.$$

Породна матриця A(X, h) може бути отримана заміною кожного елемента матриці H коду ОРС відповідним вектором-стовпцем довжини m над GF(q).

Альтернантні коди являють собою великий клас лінійних блокових кодів і узагальнюють (містять як підклас) усі розглянуті вище випадки. Справедливі наступні леми.

Лема 1. Альтернантні коди узагальнюють (містять) усі циклічні коди.

Доведення. Дійсно, довільний (n, k, d) альтернантний код A(X, h) над GF(q) складається з усіх слів коду $OPC^{\perp}_k(X, h)$ над $GF(q^m)$, таких, що їх компоненти лежать у полі GF(q). За визначенням, (n, k, d) код $OPC_k(X, h)$ складається з усіх векторів вигляду $(h_1 \cdot F(X_1), h_2 \cdot F(X_2), \dots, h_n \cdot F(X_n))$, де F(x) – будь-який многочлен з коефіцієнтами з $GF(q^m)$, степінь якого не перевищує k. Якщо $h = (h_1, h_2, \dots, h_n)$ – одиничний вектор, а вектор $X = (X_1, X_2, \dots, X_n)$ міс-

тить усі елементи $GF(q^m)$, то відповідний їм альтернантний код A(X, h) над GF(q) задається многочленом F(x), степінь якого не перевищує k. Якщо F(x) – наведений ненульовий многочлен, то, мабуть, F(x) = g(x) і, за теоремою 3, маємо (n, k, d) циклічний код над GF(q).

Лема 2. Альтернантні коди узагальнюють (містять) усі коди БЧХ.

Доведення очевидне. Коди БЧХ – підклас циклічних кодів. Якщо многочлен F(x) = g(x) (лема 1) задається виразом (3), то за теоремою 4 маємо (n, k, d) циклічний код БЧХ над GF(q).

Лема 3. Альтернантні коди узагальнюють (містять) усі коди РС.

Доведення. За визначенням, (n, k, d) альтернантний код A(X, h) над GF(q) складається з усіх слів коду $ОРС^{\perp}_k(X, h)$. Якщо $h = (h_1, h_2, \ldots, h_n)$ – одиничний вектор, вектор $X = (X_1, X_2, \ldots, X_n)$ містить усі елементи $GF(q^m)$, а многочлен $F(x) = g(x) = \prod_{i=j}^{j+2t-1} (x - \beta^i)$, то за теоремою 5 маємо (n, k, d) код РС над $GF(q^m)$.

Альтернантні коди є могутнім класом алгебраїчних лінійних блокових кодів. Найбільш значними результатами їх побудови є коди Гоппи, коди Срівестави й узагальнення Ченя-Чоя [2 – 6].

Визначення 3 [2, 4]. Альтернантний (n, k, d) код Гоппи Г(L, G) над GF(q) складається з усіх векторів $c = (c_1, c_2, \ldots, c_n)$ таких, що

$$R_c(x) \equiv 0 \bmod G(x), \qquad (6)$$

де $R_c(x) = \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i}$;

G(x) – многочлен з коефіцієнтами з $GF(q^m)$ (многочлен Гоппи);

$L = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ – підмножина елементів з $GF(q^m)$ таких, що $G(\alpha_i) \neq 0 \ \forall \alpha_i \in L$.

Використовуючи введене визначення і вираз (6), можна задати перевірочну матрицю коду Гоппи. Дійсно, многочлен $x - \alpha_i$ у кільці многочленів за модулем G(x) має зворотний многочлен

$$(x - \alpha_i)^{-1} = -\frac{G(x) - G(\alpha_i)}{x - \alpha_i} G^{-1}(\alpha_i).$$

Отже, вектор $c = (c_1, c_2, \ldots, c_n)$ належить коду Гоппи Г(L, G) тоді і тільки тоді, коли

$$\sum_{i=1}^{n} c_i \frac{G(x) - G(\alpha_i)}{x - \alpha_i} G^{-1}(\alpha_i) = 0. \qquad (7)$$

Якщо $G(x) = \sum_{i=0}^{r} g_i x^i$, де $g_i \in GF(q^m)$ і $g_r \neq 0$, то

$$\frac{G(x) - G(\alpha_i)}{x - \alpha_i} = g_r(x^{r-1} + x^{r-2}\alpha_i + \ldots + \alpha_i^{r-1}) +$$

$$+ g_{r-1}(x^{r-2}\alpha_i + \ldots + \alpha_i^{r-1}) + \ldots + g_2(x + \alpha_i) + g_1.$$

Прирівнюючи згідно з (7) нулеві всі коефіцієнти при x^{r-1}, x^{r-2}, …, 1, одержимо, що умова Hc = 0 виконається, тільки якщо

$$H = \begin{pmatrix} \begin{pmatrix} g_r G^{-1}(\alpha_1) \\ (g_{r-1} + \alpha_1 g_r) G^{-1}(\alpha_1) \\ \ldots \\ (g_1 + \alpha_1 g_2 + \ldots + \alpha_1^{r-1} g_r) G^{-1}(\alpha_1) \end{pmatrix} \\ \begin{pmatrix} g_r G^{-1}(\alpha_2) \\ (g_{r-1} + \alpha_2 g_r) G^{-1}(\alpha_2) \\ \ldots \\ (g_1 + \alpha_2 g_2 + \ldots + \alpha_2^{r-1} g_r) G^{-1}(\alpha_2) \end{pmatrix} \\ \ldots \\ \begin{pmatrix} g_r G^{-1}(\alpha_n) \\ (g_{r-1} + \alpha_n g_r) G^{-1}(\alpha_n) \\ \ldots \\ (g_1 + \alpha_n g_2 + \ldots + \alpha_n^{r-1} g_r) G^{-1}(\alpha_n) \end{pmatrix} \end{pmatrix} =$$

$$= \begin{pmatrix} g_r & 0 & \ldots & 0 \\ g_{r-1} & g_r & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ g_1 & g_2 & \ldots & g_r \end{pmatrix} \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \ldots & \alpha_n^{r-1} \end{pmatrix} \times$$

$$\times \begin{pmatrix} G^{-1}(\alpha_1) & 0 & \ldots & 0 \\ 0 & G^{-1}(\alpha_2) & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & G^{-1}(\alpha_n) \end{pmatrix}.$$

Матриця $\begin{pmatrix} g_r & 0 & \ldots & 0 \\ g_{r-1} & g_r & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ g_1 & g_2 & \ldots & g_r \end{pmatrix}$ – зворотна. Отже, перевірочна матриця

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \ldots & \alpha_n^{r-1} \end{pmatrix} \times$$

$$\times \begin{pmatrix} G^{-1}(\alpha_1) & 0 & \ldots & 0 \\ 0 & G^{-1}(\alpha_2) & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & G^{-1}(\alpha_n) \end{pmatrix} =$$

$$= \begin{pmatrix} G^{-1}(\alpha_1) & G^{-1}(\alpha_2) & \ldots & G^{-1}(\alpha_n) \\ \alpha_1 G^{-1}(\alpha_1) & \alpha_2 G^{-1}(\alpha_2) & \ldots & \alpha_n G^{-1}(\alpha_n) \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{r-1} G^{-1}(\alpha_1) & \alpha_2^{r-1} G^{-1}(\alpha_2) & \ldots & \alpha_n^{r-1} G^{-1}(\alpha_n) \end{pmatrix}$$

також задає визначений вище (n, k, d) код Гоппи Г(L, G) над GF(q).

Останній вираз при $Y = (Y_1, Y_2, \ldots, Y_n)$, $Y_1 = G^{-1}(\alpha_1)$, $Y_2 = G^{-1}(\alpha_2)$, …, $Y_n = G^{-1}(\alpha_n)$ еквівалентний виразу (5). Перевірочну матрицю $\Gamma(L, G)$ над GF(q) з елементами з GF(q) можна одержати шляхом представлення кожного елемента з $GF(q^m)$ вектором-стовпцем довжини m символів з GF(q).

Справедлива наступна теорема.

Теорема 6 [2]. Параметри (n, k, d) коду Гоппи $\Gamma(L, G)$ пов'язані співвідношеннями $n = |L|$, $k \geq n - mr$, $r = \deg G(x)$, $d \geq r + 1$. Якщо $G(x)$ – незвідний многочлен степеня r над GF(qm) і L = GF(qm), то існує код Гоппи над GF(qm) з параметрами, що лежать на межі Варшамова-Гілберта.

Теорема 6 гарантує існування хороших альтернантних кодів, побудованих через многочлен Гоппи. Водночас не існує конструктивного способу побудови хороших кодів Гоппи [2 – 6].

Іншим великим класом альтернантних кодів є узагальнені коди Срівестави.

Визначення 4 [2]. Нехай $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ і $(\beta_1, \beta_2, \ldots, \beta_s)$ – дві множини різних елементів з $GF(q^m)$ та $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ – множина ненульових елементів з $GF(q^m)$. Узагальнений (n, k, d) код Срівестави – це такий альтернантний код над GF(q), перевірочна матриця якого задається виразом (5), причому вектор $Y = (Y_1, Y_2, \ldots, Y_n)$ такий, що

$$Y_i = \frac{\gamma_i}{\prod_{j=1}^{s} (\alpha_i - \beta_j)^t}, \quad i = 1, \ldots, n... \qquad (8)$$

Справедлива наступна теорема.

Теорема 7 [2]. Параметри узагальненого (n, k, d) коду Срівестави пов'язані співвідношеннями: $k \geq n - mr$, $r = st$, $d \geq r + 1$. Блокова довжина узагальнених кодів Срівестави не перевищує $q^m - s$. Якщо $n = q^m - s$ то, за аналогією з кодами БЧХ, коди Срівестави називають примітивними.

Іншим поодиноким випадком альтернантних кодів є узагальнення Ченя-Чоя кодів БЧХ – далі узагальнені коди БЧХ (ОБЧХ).

Визначення 5 [2]. Нехай n і q взаємно прості, $GF(q^m)$ – найменше розширення поля GF(q), що містить усі корені з одиниці, P(x) і G(x) – взаємно прості з $x^n - 1$ многочлени з коефіцієнтами з $GF(q^m)$, причому $\deg(x) \leq n - 1$, $r = \deg(x) \leq n - 1$. Узагальнений код БЧХ ОБЧХ(P, G) – це такий альтернантний код над GF(q), перевірочна матриця якого задається виразом (5), причому вектор $X = (X_1, X_2, \ldots, X_n)$ складається з усіх коренів з одиниці, тобто $X = (\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{n-1})$ і вектор $Y = (Y_1, Y_2, \ldots, Y_n)$ такий, що

$$Y_i = \frac{\alpha^{i-1} \cdot p_{i-1}}{g_{i-1}}, \; I = 1, \ldots, n... \qquad (9)$$

Справедлива наступна теорема.

Теорема 8 [2]. Параметри (n, k, d) коду ОБЧХ(P, G) пов'язані співвідношеннями $k \geq n - mr$, $r = \deg(x) \leq n - 1$, $d \geq r + 1$.

Лема 4. Коди ОБЧХ(P, G) узагальнюють (містять) усі коди БЧХ.

Доведення. Очевидно, що якщо $P(x) = x^{j+2t-2}$ і $G(x) = x^{j-1}$, то код ОБЧХ(P, G) є кодом БЧХ із перевірочною матрицею вигляду (4).

Таким чином альтернантні коди є великим класом лінійних блокових кодів, що містить у собі усі циклічні коди, коди БЧХ та їх узагальнення, коди Ріда-Соломона та їх узагальнення, коди Гоппи, коди Срівестави тощо [2 – 6]. У [2, 4] показано, що при відповідному виборі вектора-шаблона $Y = (Y_1, Y_2, \ldots, Y_n)$ вдається побудувати хороші блокові коди, які лежать вище межі Варшамова-Гілберта, що узгоджується з результатом теореми 6. Однак для великих n невідоме правило вибору хороших шаблонів і, відповідно, конструктивних алгоритмів побудови хороших блокових кодів. Як показано нижче, алгебраїчні блокові коди, побудовані за алгебраїчними кривими (алгеброгеометрині коди), мають хороші конструктивні характеристики і регулярні алгоритми їх побудови.

2. Алгеброгеометричні коди. Одним з перспективних напрямків у розвитку алгебраїчної теорії кодів є методи алгеброгеометричного кодування [7 – 8]. Доведено, що при великій довжині ці коди лежать вище межі Варшамова-Гілберта [9 – 11]. У [12] наведено, що застосування алгеброгеометричних кодів для завадостійкої передачі даних дискретним каналом з незалежними помилками дозволяє одержати значний енергетичний виграш.

Зафіксуємо кінцеве поле GF(q). Нехай X – гладка проективна алгебраїчна крива в проективному просторі P^n над GF(q), $g = g(X)$ – рід кривої, X(GF(q)) – множина її точок над кінцевим полем, $N = X(GF(q))$ – їх кількість. Нехай C – клас дивізорів на X степені $\alpha > g - 1$. Тоді C визначає відображення $\varphi: X \to P^{k-1}$, де $k \geq \alpha - g + 1$. Набір $y_i = \varphi(x_i)$ задає код. Кількість точок у перетині $\varphi(X)$ з гіперплощиною дорівнює α, тобто $n - d \leq \alpha$. Ця конструкція дозволяє будувати коди з параметрами $k + d \geq n - g + 1$, довжина n яких менше або дорівнює кількості точок на кривій X. При $2g < \alpha \leq n$ алгеброгеометричний код має параметри $(n, \alpha - g + 1, d)$, $d \geq n - \alpha$. Двійковий до нього код також є алгеброгеометричним і має параметри $(n, n - \alpha + g - 1, d^{\perp})$, $d^{\perp} \geq \alpha - 2g + 2$ [7 – 8].

Дамо наступне визначення алгеброгеометричного коду.

Визначення 6 [13]. Нехай X – гладка проективна

алгебраїчна крива в проективному просторі P^n, тобто сукупність розв′язань однорідного незвідного алгебраїчного рівняння степеня degX з коефіцієнтами з GF(q). Розглянемо многостатності, що відповідають проективним гіперповерхням, заданим у P^n рівняннями F = 0, де F – однорідні одночлени степеня degF. Нехай $I(I_0, I_1, \ldots, I_{k-1})$ – інформаційна послідовність. Алгеброгеометричний код над GF(q), побудований через відображення кривої X вигляду $\varphi: EC \to P^{k-1}$ – це лінійний код довжини $n \le N$, кодові слова $C(c_0, c_1, \ldots, c_{n-1})$ якого задаються рівнянням

$$\sum_{i=0}^{k-1} I_j F_j(P_i) = c_i, \qquad (10)$$

де $P_i(X_i, Y_i, Z_i)$ – проективні точки кривої X, тобто (X_i, Y_i, Z_i) – розв′язання однорідного алгебраїчного рівняння, що задають криву X, $i = \overline{1,n}$; $F_j(P_i)$ – значення генераторних функцій у точках кривої.

Це визначення рівносильно матричному представленню алгеброгеометричного коду:

$$G\,(i_0, i_1, \ldots, i_{k-1})^T = (c_0, c_1, \ldots, c_{n-1}),$$

де
$$G = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \ldots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \ldots & F_1(P_{n-1}) \\ \ldots & \ldots & \ldots & \ldots \\ F_{k-1}(P_0) & F_{k-1}(P_1) & \ldots & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,k} - \qquad (11)$$

– породна матриця розмірності $k \times n$, $k = \alpha - g + 1$, $\alpha = \deg X \cdot \deg F$.

Визначення 7 [13]. Нехай X – гладка проективна алгебраїчна крива в P^n, тобто сукупність розв′язань однорідного незвідного алгебраїчного рівняння степеня degX з коефіцієнтами з GF(q), F – однорідні одночлени ступеня deg. Алгеброгеометричний код над GF(q) побудований через відображення кривої X вигляду $\varphi: EC \to P^{r-1}$ – це лінійний код, що складається з усіх слів $(c_0, c_1, \ldots, c_{n-1})$ довжини $n \le N$, для яких виконується рівність $d + g - 1$ рівнянь

$$\sum_{i=0}^{n-1} c_i F_j(P_i) = 0, \qquad (12)$$

де $c_i \in GF(q)$, $d \ge \alpha - 2g + 2$, $\alpha = \deg X \cdot \deg F$.

Це визначення рівносильне матричному представленню алгеброгеометричного коду

$$H\,(c_0, c_1, \ldots, c_{n-1})^T = 0,$$

де H – перевірочна матриця коду розмірності $r \times n$, $r = n - k = d + g - 2$

$$H = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \ldots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \ldots & F_1(P_{n-1}) \\ \ldots & \ldots & \ldots & \ldots \\ F_{r-1}(P_0) & F_{r-1}(P_1) & \ldots & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,r}. \qquad (13)$$

Визначення 8. Еліптичною кривою (ЕК) в афінному просторі A^2 над полем GF(q) називається гладка крива, задана рівнянням

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (14)$$

або в P^2 задана однорідним рівнянням

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3, \qquad (15)$$

де $a_i \in GF(q)$, рід кривої g = 1.

Нехай $X(GF(q))$ – множина точок гладкої проективної кривої X над кінцевим полем GF(q), $N = |X(GF(q))|$ – їх кількість. Кількість N точок кривої X над GF(q) обмежена зверху виразом Хасе-Вейля [7 – 8]

$$N \le 2\sqrt{q}\, g + q + 1, \qquad (16)$$

де g – рід кривої.

Точні значення верхньої межі кількості точок еліптичної кривої над GF(q), $q = 2m$, $m = \overline{2,10}$ наведені в табл. 1.

Таблиця 1

Оцінка верхньої межі кількості точок еліптичної проективної кривої

$GF(2^m)$	$N = \lvert EC(GF(q)) \rvert$
$GF(2^2)$	9
$GF(2^3)$	14
$GF(2^4)$	25
$GF(2^5)$	44
$GF(2^6)$	81
$GF(2^7)$	151
$GF(2^8)$	289
$GF(2^9)$	558
$GF(2^{10})$	1089

Теорема 9. Алгеброгеометричний (n, k, d) код над GF(q), побудований через відображення еліптичної кривої вигляду $\varphi: EC \to P^{k-1}$, пов'язаний характеристиками

$$k + d \ge n,$$

причому

$$\begin{cases} n \le 2\sqrt{q} + q + 1, \\ k \ge \alpha, \\ d \ge n - \alpha, \\ \alpha = 3 \cdot \deg F. \end{cases} \qquad (17)$$

Доведення. Нехай EC – гладка проективна еліптична крива в проективному просторі P^2 над GF(q), g = g(EC) = 1, EC(GF(q)) – множина її точок над GF(q), N = EC(GF(q)) – їх кількість. За теоремою Хасе-Вейля кількість точок гладкої проективної кривої роду g у P^2 над GF(q) обмежена зверху виразом $N \le 2g\sqrt{q} + q + 1$. Для еліптичної кривої цей вираз набере вигляду $N \le 2\sqrt{q} + q + 1$. За визначенням, n ≤ N, отже $n \le 2\sqrt{q} + q + 1$.

Нехай C – клас дивізорів на EC степеня α > 0. Тоді C визначає відображення φ: EC → P^{k-1}, де k ≥ α. Набір $y_i = \varphi(x_i)$ задає код. Кількість точок у перетині φ(EC) з гіперплощиною дорівнює α, тобто n – d ≤ α. Отже, параметри алгеброгеометричного коду по еліптичній кривій пов'язані співвідношенням k + d ≥ n, причому d ≥ n – α. Степінь degEC = 3, отже, α = 3degF.

Теорема 10. Алгеброгеометричний (n, k, $d^{\perp}$) код над GF(q), побудований через відображення еліптичної кривої вигляду φ: EC → P^{r-1}, пов'язаний характеристиками

$$k + d^{\perp} \ge n,$$

причому

$$\begin{cases} n \le 2\sqrt{q} + q + 1; \\ k \ge n - \alpha; \\ d^{\perp} \ge \alpha; \\ \alpha = 3\deg F. \end{cases} \qquad (18)$$

Доведення. Нехай, як і колись, EC – гладка проективна еліптична крива в проективному просторі P^2 над GF(q), g = g(EC) = 1, EC(GF(q)) – множина її точок над GF(q), N = EC(GF(q)) – їх кількість. З теореми 9 маємо $n \le 2\sqrt{q} + q + 1$. Нехай C – клас дивізорів на EC степеня α > 0. Тоді C визначає відображення φ: EC → P^{r-1}, де r ≥ α, отже, k = n – r ≥ n – α. Набір $y_i = \varphi(x_i)$ задає код. Кількість точок у перетині φ(EC) з гіперплощиною дорівнює α, тобто d ≥ α, параметри еліптичного коду пов'язані співвідношенням $k + d^{\perp} \ge n$, degEC = 3, α = 3 degF.

Визначення 9 [11]. Кривою Гурвица (Hurwitz curve) у проективному просторі P^2 над полем GF(q) називається гладка крива, задана однорідним рівнянням

$$x^m y + y^m z + z^m x = 0, \qquad (19)$$

де $q = r^3$, r – позитивне ціле число, характеристика поля GF(q) ділиться на $m^2 - m + 1$.

Рід такої кривої визначається з рівняння

$$g = \frac{(q^{1/3} + 1)q^{1/3}}{2}. \qquad (20)$$

Кількість точок кривої Гурвіца нижче межі Хасе-Вейля і визначається виразом вигляду

$$N = q + 2q^{2/3} + 2q^{1/3} + 1. \qquad (21)$$

Точні значення верхньої межі кількості точок кривої Гурвіца над GF(q), q = 2m, $m = \overline{2, 10}$ наведені в табл. 2.

Таблиця 2

Оцінка верхньої межі кількості точок кривої Гурвіца

$GF(2^m)$	$N = \lvert EC(GF(q)) \rvert$
$GF(2^3)$	21
$GF(2^6)$	105
$GF(2^9)$	197

Теорема 11. Алгеброгеометричний (n, k, d) код над GF(q), побудований через відображення кривої Гурвіца вигляду φ: HurC → P^{k-1}, пов'язаний характеристиками

$$k + d \ge n - \frac{(q^{1/3} + 1)q^{1/3}}{2} + 1,$$

причому

$$\begin{cases} n \le q + 2q^{2/3} + 2q^{1/3} + 1; \\ k \ge \alpha - \dfrac{(q^{1/3} + 1)q^{1/3}}{2} + 1; \\ d \ge n - \alpha; \\ \alpha = (m + 1)\deg F. \end{cases} \qquad (22)$$

Доведення. Нехай Hur – гладка проективна крива Гурвіца в проективному просторі P^2 над GF(q), $g = g(HurC) = \frac{(q^{1/3} + 1)q^{1/3}}{2}$, HurCGF(q)) – множина її точок над GF(q), $N = \lvert HurC(GF(q)) \rvert$ – їх кількість. Для кривої Гурвіца $N = q + 2q^{2/3} + 2q^{1/3} + 1$. За визначенням n ≤ N, отже $n \le q + 2q^{1/3} + 2q^{1/3} + 1$.

Нехай C – клас дивізорів на HurC степеня α > 0. Тоді C визначає відображення φ: HurC→ P^{k-1}, де $k \ge \alpha - \frac{(q^{1/3} + 1)q^{1/3}}{2} + 1$. Набір $y_i = \varphi(x_i)$ задає код. Кількість точок у перетині φ(HurC) з гіперплощиною дорівнює α, тобто n – d ≤ α. Отже параметри алгеброгеометричного коду за кривою Ерміта пов'язані співвідношенням $k + d \ge n - \frac{(q^{1/3} + 1)q^{1/3}}{2} + 1$, причому d ≥ n – α. Степінь degHurC = m + 1, отже α = (m + 1)degF.

Теорема 12. Алгеброгеометричний $(n, k, d^{\perp})$ код над GF(q), побудований через відображення кривої Гурвіца вигляду φ: HurC $\to P^{r-1}$ пов'язаний характеристиками

$$k + d^{\perp} \ge n - \frac{(q^{1/3}+1)q^{1/3}}{2} + 1,$$

причому

$$\begin{cases} n \le q + 2q^{2/3} + 2q^{1/3} + 1; \\ k \ge n - \alpha + \frac{(q^{1/3}+1)q^{1/3}}{2} - 1; \\ d^{\perp} \ge \alpha - (q^{1/3}+1)q^{1/3} + 2; \\ \alpha = \left(\sqrt{q}+1\right)\deg F. \end{cases} \qquad (23)$$

Доведення. Нехай, як і колись, HurC – гладка проективна крива Гурвіца в проективному просторі P^2 над GF(q),

$$g = g(\text{HurC}) = \frac{(q^{1/3}+1)q^{1/3}}{2},$$

де HurC(GF(q)) – множина її точок над GF(q), $N = |\text{HurC}(\text{GF}(q))|$ – їх кількість. З теореми 11 маємо $n \le q + 2q^{2/3} + 2q^{1/3} + 1$. Нехай C – клас дивізорів на HurC степеня $\alpha > 0$. Тоді C визначає відображення φ: HurC $\to P^{r-1}$, де $r \ge \alpha - \frac{(q^{1/3}+1)q^{1/3}}{2} + 1$, отже $k = n - r \ge n - \alpha + \frac{(q^{1/3}+1)q^{1/3}}{2} - 1$. Набір $y_i = \varphi(x_i)$ задає код. Кількість точок у перетині φ(HurC) з гіперплощиною дорівнює α, тобто $d^{\perp} \ge \alpha - (q^{1/3}+1)\times$ $\times q^{1/3} + 2$, параметри коду за кривою Гурвіца пов'язані співвідношенням:

$$k + d^{\perp} \ge n - \frac{(q^{1/3}+1)q^{1/3}}{2} + 1,$$

$$\deg \text{HurC} = m + 1, \quad \alpha = (m+1)\deg F.$$

Визначення 10 [7 – 8, 11]. Кривою Ерміта (Hermit curve) у проективному просторі P^2 над полем GF(q) називається гладка крива, задана однорідним рівнянням

$$x^{\sqrt{q}+1} + y^{\sqrt{q}+1} + z^{\sqrt{q}+1} = 0, \qquad (24)$$

де $q = r^2$, r – позитивне ціле число.

Рід такої кривої визначається виразом вигляду

$$g = \frac{q - \sqrt{q}}{2}. \qquad (25)$$

Кількість точок задовольняє верхню межу Хасе-Вейля і визначається виразом вигляду

$$N = q\sqrt{q} + 1. \qquad (26)$$

Точні значення верхньої межі кількості точок кривої Ерміта над GF(q), $q = 2m$, $m = \overline{2, 10}$ наведені в табл. 3.

Таблиця 3

Оцінка верхньої межі кількості точок кривої Ерміта

$GF(2^m)$	$N = \lvert EC(GF(q)) \rvert$
$GF(2^2)$	9
$GF(2^4)$	65
$GF(2^6)$	513
$GF(2^8)$	4097
$GF(2^{10})$	32769

У ході проведених досліджень [11] виділено клас кривих (27) – (29), що дають $N = q\sqrt{q} + 1$ розв′язань над полем GF(q), $q = r^2$, r – позитивне ціле число, при роді $g = \left(q - \sqrt{q}\right)/2$:

$$x^{\sqrt{q}+1} + y^{\sqrt{q}}z + yz^{\sqrt{q}} = 0; \qquad (27)$$

$$x^{\sqrt{q}+1} + x^{\sqrt{q}}y + x^{\sqrt{q}}z + xy^{\sqrt{q}} + xz^{\sqrt{q}} + y^{\sqrt{q}+1} = 0; \qquad (28)$$

$$x^{\sqrt{q}+1} + x^{\sqrt{q}}y + x^{\sqrt{q}}z + xy^{\sqrt{q}} + xz^{\sqrt{q}} + y^{\sqrt{q}+1} + z^{\sqrt{q}+1} = 0. \qquad (29)$$

Дослідження властивостей точок цих кривих показали, що в полях $GF(2^m)$, m = 2, 4, 6, 8, 10 криві, задані рівняннями (27) – (29) дають кількість точок $N = q\sqrt{q} + 1$, яка відповідає кількості точок кривої Ерміта. Рід кривих (27) – (29), кількість точок та алгебраїчний степінь еквівалентні відповідним показникам кривої Ерміта. Проведені дослідження властивостей точок кривих (27) – (29) показали, що $N = q\sqrt{q}$ розв′язань однозначно задаються набором P(X, Y, 1). Подібна форма дозволяє спростити процедуру обчислення генераторних функцій у точках кривої. При укороченні на один символ коду для обчислення значення генераторних функцій у точках кривих (27) – (29) необхідно виконати дві операції піднесення до степеня й одну операцію множення.

Теорема 13. Алгеброгеометричний (n, k, d) код над GF(q), побудований через відображення кривої Ерміта вигляду φ: HC $\to P^{k-1}$, пов'язаний характеристиками

$$k + d \ge n - \frac{q - \sqrt{q}}{2} + 1,$$

причому

$$\begin{cases} n \le q\sqrt{q}+1; \\ k \ge \alpha - \dfrac{q-\sqrt{q}}{2}+1; \\ d \ge n-\alpha; \\ \alpha = \left(\sqrt{q}+1\right)\deg F. \end{cases} \quad (30)$$

Доведення. Нехай HC – гладка проективна крива Ерміта в проективному просторі P^2 над GF(q), $g = g(HC) = \dfrac{q-\sqrt{q}}{2}$, HC(GF(q)) – множина її точок над GF(q), N = HC(GF(q)) – їх кількість. Для кривої Ерміта $N = q\sqrt{q}+1$. За визначенням $n \le N$, отже $n \le q\sqrt{q}+1$.

Нехай C – клас дивізорів на HC степеня $\alpha > 0$. Тоді C визначає відображення $\varphi: HC \to P^{k-1}$, де $k \ge \alpha - \dfrac{q-\sqrt{q}}{2}+1$. Набір $y_i = \varphi(x_i)$ задає код. Кількість точок у перетині $\varphi(HC)$ з гіперплощиною дорівнює α, тобто $n - d \le \alpha$. Отже параметри алгеброгеометричного коду по кривій Ерміта пов'язані співвідношенням $k + d \ge n - \dfrac{q-\sqrt{q}}{2}+1$, причому $d \ge n - \alpha$. Степінь $\deg HC = \sqrt{q}+1$, отже $\alpha = \left(\sqrt{q}+1\right)\deg F$.

Теорема 14. Алгеброгеометричний $(n, k, d^{\perp})$ код над GF(q), побудований через відображення кривої Ерміта вигляду $\varphi: HC \to P^{r-1}$, пов'язаний характеристиками

$$k + d^{\perp} \ge n - \frac{q-\sqrt{q}}{2}+1,$$

причому

$$\begin{cases} n \le q\sqrt{q}+1; \\ k \ge n - \alpha + \dfrac{q-\sqrt{q}}{2} - 1; \\ d^{\perp} \ge \alpha - q + \sqrt{q} + 2; \\ \alpha = \left(\sqrt{q}+1\right)\deg F. \end{cases} \quad (31)$$

Доведення. Як і раніше, HC – гладка проективна крива Ерміта в проективному просторі P^2 над GF(q), $g = g(HC) = \dfrac{q-\sqrt{q}}{2}$, HC(GF(q)) – множина її точок над GF(q), N = HC(GF(q)) – їх кількість. З теореми 13 маємо $n \le q\sqrt{q}+1$. Нехай C – клас дивізорів на HC степеня $\alpha > 0$. Тоді C визначає відображення $\varphi: HC \to P^{r-1}$, де $r \ge \alpha - \dfrac{q-\sqrt{q}}{2}+1$, отже $k = n - r \ge n - \alpha + \dfrac{q-\sqrt{q}}{2} - 1$. Набір $y_i = \varphi(x_i)$ задає код. Кількість точок у перетині $\varphi(HC)$ з гіперплощиною дорівнює α, тобто $d^{\perp} \ge \alpha - q + \sqrt{q} + 2$, параметри еліптичного коду пов'язані співвідношенням $k + d^{\perp} \ge n - \dfrac{q-\sqrt{q}}{2}+1$, $\deg HC = \sqrt{q}+1$, $\alpha = \left(\sqrt{q}+1\right)\deg F$.

Визначення 11 [11]. Кривою Ферма (Ferma curve) у проективному просторі P^2 над полем GF(q) називається гладка крива, задана однорідним рівнянням

$$x^{q^{2/3}+q^{1/3}+1} + x^{q^{2/3}+q^{1/3}+1} + x^{q^{2/3}+q^{1/3}+1} = 0, \quad (32)$$

де $q = r^3$, r – позитивне ціле число.

Рід такої кривої визначається виразом вигляду

$$g = \frac{q^{4/3} + 2q - q^{1/3}}{2}. \quad (33)$$

Кількість точок кривої Ферма нижче межі Хасе-Вейля і визначається виразом вигляду

$$N = q^{5/3} - q - q^{2/3} + 1. \quad (34)$$

Точні значення верхньої межі кількості точок кривої Ферма над GF(q), $q = 2m$, $m = \overline{2,10}$ наведені в табл. 4.

Таблиця 4

Оцінка верхньої межі кількості точок кривої Ферма

$GF(2^m)$	$N = \lvert EC(GF(q))\rvert$
$GF(2^3)$	27
$GF(2^6)$	945
$GF(2^9)$	32193

Теорема 15. Алгеброгеометричний (n, k, d) код над GF(q), побудований через відображення кривої Ферма вигляду $\varphi: FC \to P^{k-1}$, зв'язаний характеристиками

$$k + d \ge n - \frac{q^{4/3} + 2q - q^{1/3}}{2}+1,$$

причому

$$\begin{cases} n \le q^{5/3} - q - q^{2/3} + 1; \\ k \ge \alpha - \dfrac{q^{4/3} + 2q - q^{1/3}}{2} + 1; \\ d \ge n - \alpha; \\ \alpha = \left(q^{2/3} + q^{1/3} + 1\right)\deg F. \end{cases} \quad (35)$$

Доведення. Нехай FC – гладка проективна крива Ферма в проективному просторі P^2 над GF(q),

$g = g(FC) = \dfrac{q^{4/3} + 2q - q^{1/3}}{2}$, FC(GF(q)) – множина її точок над GF(q), $N = |FC(GF(q))|$ – їх кількість. Для кривої Ферма $N = q^{5/3} - q - q^{2/3} + 1$. За визначенням $n \le N$, отже $n \le q^{5/3} - q - q^{2/3} + 1$.

Нехай C – клас дивізорів на FC степеня $\alpha > 0$. Тоді C визначає відображення $\varphi: FC \to P^{k-1}$, де $k \ge \alpha - \dfrac{q^{4/3} + 2q - q^{1/3}}{2} + 1$. Набір $y_i = \varphi(x_i)$ задає код. Кількість точок у перетині $\varphi(FC)$ з гіперплощиною дорівнює α, тобто $n - d \le \alpha$. Отже параметри алгеброгеометричного коду по кривій Ферма пов'язані співвідношенням $k + d \ge n - \dfrac{q^{4/3} + 2q - q^{1/3}}{2} + 1$, причому $d \ge n - \alpha$. Степінь $\deg FC = q^{2/3} + q^{1/3} + 1$, отже, $\alpha = \left(q^{2/3} + q^{1/3} + 1\right)\deg F$.

Теорема 16. Алгеброгеометричний $(n, k, d^{\perp})$ код над GF(q), побудований через відображення кривої Ферма вигляду $\varphi: FC \to P^{r-1}$, пов'язаний характеристиками

$$k + d^{\perp} \ge n - \frac{q^{4/3} + 2q - q^{1/3}}{2} + 1,$$

причому

$$\begin{cases} n \le q^{5/3} - q - q^{2/3} + 1; \\ k \ge n - \alpha + \dfrac{q^{4/3} + 2q - q^{1/3}}{2} - 1; \\ d^{\perp} \ge \alpha - q^{4/3} - 2q + q^{1/3} + 2; \\ \alpha = \left(q^{2/3} + q^{1/3} + 1\right)\deg F. \end{cases} \qquad (36)$$

Доведення. Нехай, як і раніше, FC – гладка проективна крива Ферма в проективному просторі P^2 над GF(q), $g = g(FC) = \dfrac{q^{4/3} + 2q - q^{1/3}}{2}$, FC(GF(q)) – множина її точок над GF(q), $N = |FC(GF(q))|$ – їх кількість. З теореми 15 маємо $n \le q^{5/3} - q - q^{2/3} + 1$. C – клас дивізорів на FC степеня $\alpha > 0$. Тоді C визначає відображення $\varphi: FC \to P^{r-1}$, де $r \ge \alpha - \dfrac{q^{4/3} + 2q - q^{1/3}}{2} + 1$, отже, $k = n - r \ge n - \alpha + \dfrac{q^{4/3} + 2q - q^{1/3}}{2} - 1$. Набір $y_i = \varphi(x_i)$ задає код. Кількість точок у перетині $\varphi(FC)$ з гіперплощиною дорівнює α, тобто $d^{\perp} \ge \alpha - q^{4/3} - 2q + q^{1/3} + 2$, параметри коду за кривою Ферма зв'язані співвідношенням $k + d^{\perp} \ge n - \dfrac{q^{4/3} + 2q - q^{1/3}}{2} + 1$, $\deg FC = q^{2/3} + q^{1/3} + 1$, $\alpha = \left(q^{2/3} + q^{1/3} + 1\right) \cdot \deg F$.

Визначення 12 [11]. Кривою Сузукі (Susuki curve) у проективному просторі P^2 над полем GF(q) називається гладка крива, задана однорідним рівнянням

$$x^{q_0}(z^q + zx^{q-1}) + y^{q_0}(y^q + yx^{q-1}) = 0, \qquad (37)$$

де $q = 2^{2f+1}$, $q_0 = 2^f$;

f – позитивне ціле число.

Рід такої кривої визначається виразом вигляду

$$g = \frac{q^2 - q}{\left\lfloor 2\sqrt{q} \right\rfloor}. \qquad (38)$$

Кількість точок кривої Сузукі нижче межі Хасе-Вейля і визначається виразом вигляду

$$N = q^2 + 1. \qquad (39)$$

Точні значення верхньої межі кількості точок кривої Сузукі над GF(q), $q = 2m$, $m = \overline{2,10}$ наведені в табл. 5.

Таблиця 5

Оцінка верхньої межі кількості точок кривої Сузукі

$GF(2^m)$	$N = \lvert EC(GF(q)) \rvert$
$GF(2^2)$	17
$GF(2^3)$	65
$GF(2^4)$	257
$GF(2^5)$	1025
$GF(2^6)$	4097
$GF(2^7)$	16385
$GF(2^8)$	65537
$GF(2^9)$	262145
$GF(2^{10})$	1048577

У ході проведених досліджень виділено клас кривих (40) – (42), що дають $N = q^2 + 1$ розв′язань над полем GF(q) при роді $g = \dfrac{q^2 - q}{\left\lfloor 2\sqrt{q} \right\rfloor}$:

$$x^{q-1}y^2 + y^{q+1} + x^q z + xz^q; \qquad (40)$$

$$x^q y + x^{q-1}y^2 + xy^q + y^{q+1} + x^q z + xz^q; \qquad (41)$$

$$x^{q+1} + y^{q+1} + z^{q-1}x^2 + z^{q-1}y^2 + \\ + x^q y + xy^q + x^q z + xz^q. \qquad (42)$$

Дослідження властивостей точок цих кривих, проведені в роботі, показали, що в полях $GF(2^m)$,

m = 2, 4, 6, 8, 10, криві, задані рівняннями (40) – (42) дають кількість точок $N = q^2 + 1$, що відповідає кількості точок кривої Сузукі. Очевидно, рід кривих (40) – (42), кількість точок та алгебраїчний степінь еквівалентні відповідним показникам кривої Сузукі, заданої виразом (37).

Теорема 17. Алгеброгеометричний (n, k, d) код над GF(q), побудований через відображення кривої Сузукі вигляду $\varphi: SC \to P^{k-1}$, пов'язаний характеристиками

$$k + d \ge n - \frac{q^2 - q}{\lfloor 2\sqrt{q} \rfloor} + 1,$$

причому

$$\begin{cases} n \le q^2 + 1; \\ k \ge \alpha - \dfrac{q^2 - q}{\lfloor 2\sqrt{q} \rfloor} + 1; \\ d \ge n - \alpha; \\ \alpha = (q+1)\deg F. \end{cases} \quad (43)$$

Доведення. Нехай SC – гладка проективна крива Сузукі в проективному просторі P^2 над GF(q), $g = g(SC) = \dfrac{q^2 - q}{\lfloor 2\sqrt{q} \rfloor}$, SC(GF(q)) – множина її точок над GF(q), $N = |SC(GF(q))|$ – їх кількість. Для кривої Сузукі $N = q^2 + 1$. За визначенням $n \le N$, отже $n \le q^2 + 1$.

Припустимо, що C – клас дивізорів на SC степеня $\alpha > 0$. Тоді C визначає відображення $\varphi: SC \to P^{k-1}$, де $k \ge \alpha - \dfrac{q^2 - q}{\lfloor 2\sqrt{q} \rfloor} + 1$. Набір $y_i = \varphi(x_i)$ задає код. Кількість точок у перетині $\varphi(SC)$ з гіперплощиною дорівнює α, тобто $n - d \le \alpha$. Отже параметри алгеброгеометричного коду по кривій Ферма пов'язані співвідношенням $k + d \ge n - \dfrac{q^2 - q}{\lfloor 2\sqrt{q} \rfloor} + 1$, причому $d \ge n - \alpha$. Степінь $\deg SC = q + 1$, отже $\alpha = (q+1)\deg F$.

Теорема 18. Алгеброгеометричний $(n, k, d^{\perp})$ код над GF(q), побудований через відображення кривої Сузукі вигляду $\varphi: SC \to P^{r-1}$, зв'язаний характеристиками

$$k + d^{\perp} \ge n - \frac{q^2 - q}{\lfloor 2\sqrt{q} \rfloor} + 1,$$

причому

$$\begin{cases} n \le q^2 + 1; \\ k \ge n - \alpha + \dfrac{q^2 - q}{\lfloor 2\sqrt{q} \rfloor} - 1; \\ d^{\perp} \ge \alpha - \dfrac{q^2 - q}{\lfloor \sqrt{q} \rfloor} + 2; \\ \alpha = (q+1)\deg F. \end{cases} \quad (44)$$

Доведення. Нехай, як і раніше, SC – гладка проективна крива Ферма в проективному просторі P^2 над GF(q), $g = g(SC) = \dfrac{q^2 - q}{\lfloor 2\sqrt{q} \rfloor}$, SC(GF(q)) – множина її точок над GF(q), $N = |SC(GF(q))|$ – їх кількість. З теореми 17 маємо $n \le q^2 + 1$. Нехай C – клас дивізорів на SC степеня $\alpha > 0$. Тоді C визначає відображення $\varphi: SC \to P^{r-1}$, де $r \ge \alpha - \dfrac{q^2 - q}{\lfloor 2\sqrt{q} \rfloor} + 1$, отже $k = n - r \ge n - \alpha + \dfrac{q^2 - q}{\lfloor 2\sqrt{q} \rfloor} - 1$. Набір $y_i = \varphi(x_i)$ задає код. Кількість точок у перетині $\varphi(SC)$ з гіперплощиною дорівнює α, тобто $d^{\perp} \ge \alpha - \dfrac{q^2 - q}{\lfloor \sqrt{q} \rfloor} + 2$, параметри коду по кривій Сузукі пов'язані співвідношенням $k + d^{\perp} \ge n - \dfrac{q^2 - q}{\lfloor 2\sqrt{q} \rfloor} + 1$, $\deg SC = q + 1$, $\alpha = (q+1)\deg F$.

3. Теоретичне узагальнення найбільш важливих лінійних блокових кодів. Дослідимо зв'язок алгеброгеометричних і альтернантних кодів, методи побудови узагальнених кодів РС і альтернантних кодів через алгеброгеометричні коди.

Як показали проведені дослідження, код Рида-Соломона можна представити як код, побудований за проективною прямою. Його алгеброгеометричне узагальнення задається такою теоремою.

Теорема 19. Алгеброгеометричний код, побудований по проективній прямій над GF(q), визначає код РС.

Доведення. Дійсно, нехай X – проективна пряма над GF(q). Рід проективної прямої $g = g(X) = 0$, X(GF(q)) – множина її точок над GF(q), $N = |X(GF(q))|$ – їх кількість, N = q + 1. Точки прямої визначаються гомогенними координатами (x, y) та мають значення $P_i = (\alpha_i, 1)$, $0 \le i \le q - 1$ і

$Q = (1,0)$ – особлива точка (точка невизначеності).

Нехай C – клас дивізорів на X степені $\alpha > 0$. Тоді C визначає відображення $\varphi: X \to P^{k-1}$, де $k \ge \alpha + 1$. Набір $y_i = \varphi(x_i)$ задає (n, k, d) код. Кількість точок у перетині $\varphi(X)$ з гіперплощиною дорівнює α, тобто $n - d \le \alpha$. Отже $n \le N$, $k \ge \alpha + 1$, $d \ge n - \alpha$, $\alpha = \deg F$. Якщо C визначає відображення $\varphi: X \to P^{r-1}$, де $r \ge \alpha + 1$, то $y_i = \varphi(x_i)$ задає код $(n, k, d^{\perp})$ з параметрами $n \le N$, $k \ge n - \alpha - 1$, $d^{\perp} \ge \alpha + 2$, $\alpha = \deg F$. Параметри алгеброгеометричного коду за проективною прямою пов'язані співвідношенням $k + d \ge n + 1$, що відповідають коду РС.

Висновок 1. Якщо алгеброгеометричний код будується через відображення точок $P_i = (\alpha_i, 1)$, $1 \le i \le q - 1$, то код визначається як

$$C = \left\{ (F(P_1), \ldots, F(P_{q-1})) \middle| F \in Z \right\},$$

де Z – множина раціональних функцій на X, що визначені в кожній точці і мають полюс порядку менше α. Очевидно, що це код РС із (n, k, d) параметрами $(q - 1, \alpha, q - 1 - \alpha)$.

Висновок 2. Якщо алгеброгеометричний код будується через відображення точок $P_i = (\alpha_i, 1)$, $0 \le i \le q - 1$, то код визначається як

$$C = \left\{ (F(P_0), F(P_1), \ldots, F(P_{q-1})) \middle| F \in Z \right\},$$

і маємо розширений на один символ код РС із (n, k, d) параметрами: $(q, \alpha, q - \alpha)$.

Висновок 3. Якщо алгеброгеометричний код будується через відображення точок $Q = (1, 0)$, $P_i = (\alpha_i, 1)$, $0 \le i \le q - 1$, то код визначається як

$$C = \left\{ (F(Q), F(P_0), F(P_1), \ldots, F(P_{q-1})) \middle| F \in Z \right\},$$

і маємо розширений на два символи код РС із (n, k, d) параметрами $(q + 1, \alpha, q + 1 - \alpha)$.

Результат теореми 19 та її висновки установлюють важливий зв'язок між великими класами альтернантних і алгеброгеометричних кодів. Дійсно, у визначенні альтернантних кодів використовується породна матриця узагальненого коду РС (визначення 1, 2). Використовуючи узагальнення кодів РС, побудованих через відображення проективної прямої (алгеброгеометричний код з теореми 19), одержимо необхідний інструмент для побудови довільного альтернантного коду.

Справедлива така теорема.

Теорема 20. Узагальнений код РС, заданий перевірочною матрицею вигляду (5), однозначно задається алгеброгеометричним кодом, побудованим через відображення проективної прямої.

Доведення. Дійсно, якщо точки проективної прямої представити у вигляді пар (x, y), то відображення C з теореми 19 породжує генераторну матрицю (права частина виразу (5)). Якщо C визначає відображення $\varphi: X \to P^{r-1}$, де $r \ge \alpha + 1$, то $y_i = Y_i \cdot \varphi(x_i)$ задає $(n, k, d^{\perp})$ код ОРС із перевірочною матрицею вигляду (5). Справедливі також висновки 1 – 3 теореми 19, що задають розширені коди ОРС.

Результат останньої теореми дозволяє визначити код ОРС через відображення проективної прямої, тобто задавати перевірочну матрицю ОРС коду за допомогою генераторної матриці алгеброгеометричного коду. Справедливо також узагальнення всього класу альтернантних кодів, що задається такою теоремою.

Теорема 21. Альтернантний код, заданий обмеженням коду ОРС, однозначно задається відповідним обмеженням алгеброгеометричного коду, побудованого через відображення проективної прямої.

Доведення. За визначенням 2, альтернантний код над GF(q) складається з усіх слів коду ОРС над $GF(q^m)$ таких, що їх компоненти лежать у полі GF(q), тобто дорівнює обмеженню коду ОРС на підполі GF(q). При побудові перевірочної матриці альтернантного коду над GF(q) кожен символ генераторної матриці заміняється вектором-стовпцем довжини m символів з GF(q). За теоремою 20, код ОРС над $GF(q^m)$ однозначно задається алгеброгеометричним кодом над $GF(q^m)$, побудованим по проективній прямій. Отже, генераторна матриця алгеброгеометричного коду задає перевірочну матрицю ОРС коду, яка у свою чергу задає перевірочну матрицю альтернантного коду.

Висновок 1. Будь-який циклічний код над GF(q) може бути заданий відповідним обмеженням алгеброгеометричного коду, заданого над $GF(q^m)$.

Доведення. За лемою 1 альтернантні коди узагальнюють (містять) усі циклічні коди. За теоремою 20 альтернантний код задається обмеженням алгеброгеометричного коду. Отже існує відповідне обмеження алгеброгеометричного коду, що породжує довільний циклічний код.

Висновок 2. Будь-який код БЧХ над GF(q) може бути заданий відповідним обмеженням алгеброгеометричного коду, заданого над $GF(q^m)$.

Доведення аналогічне доведенню висновка 1. Коди БЧХ – підклас циклічних кодів. Отже за теоремою 20 і лемою 2 існує відповідне обмеження алгеброгеометричного коду, що породжує довільний код БЧХ.

Висновок 3. Довільний код Гоппи над GF(q) може бути заданий відповідним обмеженням алгеброгеометричного коду, заданого над $GF(q^m)$.

Доведення. За визначенням 3, кодом Гоппи є альтернантний код з $Y = (Y_1, Y_2, \ldots, Y_n)$, $Y_1 = G^{-1}(\alpha_1)$, $Y_2 = G^{-1}(\alpha_2)$, …, $Y_n = G^{-1}(\alpha_n)$ у виразі (5).

Представимо точки проективної прямої у вигляді пар (x = 1, y), причому $y_1 = Y_1$, $y_2 = Y_2$, …, $y_n = Y_n$... Тоді генераторна матриця алгеброгеометричного коду, побудованого через відповідне відображення проективної прямої, однозначно задає перевірочну матрицю ОРС коду, обмеження якого задає шуканий альтернантний код Гоппи.

Висновок 4. Довільний код Срівестави над GF(q) може бути заданий відповідним обмеженням алгеброгеометричного коду, заданого над $GF(q^m)$.

Доведення аналогічне доведенню висновку 3.

Висновок 5. Довільний код ОБЧХ над GF(q) може бути заданий відповідним обмеженням алгеброгеометричного коду, заданого над $GF(q^m)$.

Доведення аналогічне доведенню висновку 3.

Використовуючи викладений вище підхід до опису альтернантних кодів, введемо новий клас алгебраїчних блокових кодів. Скористаємося введеним визначенням алгеброгеометричного коду $GF(q^m)$. З кодових слів цього коду задамо лінійний підпростір у $GF^n(q)$. Введемо наступне визначення.

Визначення 12. Зрізаний алгеброгеометричний (n, k, d) код над GF(q) складається з усіх слів коду алгеброгеометричного (N, K, D) коду над $GF(q^m)$ таких, що їх компоненти лежать у полі GF(q). Іншими словами, зрізаний код дорівнює обмеженню вихідного коду на підполі GF(q), а перевірочна матриця зрізаного коду може бути отримана заміною кожного елемента перевірочної матриці алгеброгеометричного коду відповідним вектором-стовпцем довжини m над GF(q).

Таким чином, кодові слова зрізаного коду складаються з усіх векторів X над GF(q), що задовольняють рівнянню

$$H \cdot X^T = 0,$$

де H – перевірочна матриця алгеброгеометрического (N, K, D) коду над $GF(q^m)$.

Справедлива наступна теорема.

Теорема 1. Параметри зрізаного (n, k, d) коду зв'язані співвідношеннями

$$n = N;$$

$$N - m(N - K) \le k \le K;$$

$$d \ge D.$$

Доведення. Визначений вище зрізаний код є обмеженням алгеброгеометричного (N, K, D) коду над $GF(q^m)$ на підполі GF(q), що у свою чергу є підпростором $GF^K(q)$ простору $GF^N(q)$. Практично це означає, що кодові слова зрізаного коду над GF(q) належать (N, K, D) кодові над $GF(q^m)$ та є векторами з $GF^N(q)$, тобто n = N. Обмеження (N, K, D) коду над $GF(q^m)$ на підполі GF(q) не збільшує розмірність підпростору $GF^K(q)$, тобто $k \le K$. Водночас обмеження алгеброгеометричного коду через заміну кожного елемента його перевірочної матриці на вектор-стовпець довжини m над GF(q) може привести до зменшення розмірності коду. У результаті такої заміни (N – K) рядків матриці H перетворяться в m(N – K) рядків, що зададуть базис лінійного простору $GF^r(q)$ розмірності $L \le m(N - K)$. З умови взаємної ортогональності елементів $GF^r(q)$ і $GF^k(q)$ маємо $n - m(N - K) \le k$, звідси $N - m(N - K) \le k$. І, нарешті, відображення елементів з $GF(q^m)$ в елементи GF(q) не зменшує ваги векторів з $GF^k(q)$, отже $d \ge D$.

Кожен лінійний (n, k, d) код над GF(q) є підпростором $GF^k(q)$ простору $GF^n(q)$.

Породна матриця зрізаного коду може бути отримана заміною кожного елемента перевірочної матриці алгеброгеометричного коду відповідним вектором-стовпцем довжини m над GF(q).

4. Алгоритми кодування алгеброгеометричними кодами та їх підкодами. У [13] пропонуються способи систематичного і несистематичного кодування, що дозволяють формувати кодові слова для довільних k символів повідомлення і припускаючих практичну реалізацію кодів по довільній кривій у P^2 над GF(q). Складність реалізації знижена на 30 % за рахунок побудови генераторної матриці коду відображенням тільки точок кривої вигляду P(X, Y, 1).

Розглянемо криву X у P^2 над GF(q) , а також многостатності, що відповідають проективним гіперповерхням, заданим у P^2 рівняннями $F = 0$, де F – однорідні одночлени.

При систематичному кодуванні скористаємося визначенням алгеброгеометричного коду, побудованого через перевірочну матрицю.

Систематичний спосіб алгеброгеометричного кодування полягає в наступному [13]. Нехай I – множина k інформаційних позицій кодового слова (тобто множина номерів позицій, що входять у заданий інформаційний набір коду) і h – множина r = n – k перевірочних позицій. Об'єднання множин $I \cup h$ містить усі цілі числа (номери) від 0 до n – 1. На інформаційних позиціях розмістимо k символів повідомлення, а на перевірочних – нулі. Обчислимо суми

$$S_j = \sum_{i \in I} c_i F_j(P_i), \quad j = \overline{0, r-1}$$

або в матричній формі

$$\left\| S_j \right\|_r = \left\| F_j(P_i) \right\|_{k,r} \left\| c_i \right\|_k^T. \qquad (45)$$

Завдання полягає в тому, щоб обчислити і записати на перевірочних позиціях такі символи c_i, $i \in h$, що задовольняють рівнянню (11). З визначення алгеброгеометричного коду випливає, що значення

$r = n - k$ перевірочних символів можуть бути знайдені із системи лінійних рівнянь

$$\sum_{i \in h} c_i F_j(P_i) = -S_j, \quad j = \overline{0, r-1}.$$

У матричному представленні останній запис еквівалентний виразу

$$\left\| F_j(P_i) \right\|_{r,r} \left\| c_i \right\|_r^T = \left\| - S_j \right\|_r .$$

Для знаходження значень $r = n - k$ перевірочних символів можна використовувати методи зворотних матриць [13]. Запишемо в матричній формі

$$\left\| c_i \right\|_r = \left\| F_j(P_i) \right\|_{r,r}^{-1} \left\| - S_j \right\|_r^T , \qquad (46)$$

де $\left\| F_j(P_i) \right\|_{r,r}^{-1}$ – зворотна матриця;

$$\left\| F_j(P_i) \right\|_{r,r}^{-1} = \left\| \frac{A\left[F_j(P_i)\right]}{\Delta} \right\|_{r,r} ;$$

$A\left[F_j(P_i)\right]$ – алгебраїчне доповнення елемента $F_j(P_i)$;

Δ – визначник матриці $\left\| F_j(P_i) \right\|_{r,r}$.

Оскільки розміщення перевірочних позицій звичайно відомо і фіксовано, то заздалегідь можна знайти зворотну матрицю для системи рівнянь (11) і одержати всі перевірочні символи множенням вектора $(S_0, S_1, \ldots, S_{r-1})$ на матрицю $\left\| F_j(P_i) \right\|_{r,r}^{-1}$.

Як інформаційні можуть бути обрані будь-які k позицій кодового слова. Отже завжди можна вибрати таку множину перевірочних (та інформаційних) позицій, для якої матриця $\left\| F_j(P_i) \right\|_{r,r}^{-1}$ найбільш зручна в обчисленні.

Таким чином, для реалізації систематичного способу алгеброгеометричного кодування досить зберігати елементи матриць $\left\| F_j(P_i) \right\|_{k,r}$ і $\left\| F_j(P_i) \right\|_{r,r}^{-1}$ або по черзі обчислювати $\left\| F_j(P_i) \right\|_{k,r}$ як значення генераторних функцій у точках кривої.

Алгоритм систематичного кодування задамо у вигляді послідовності наступних кроків.

Крок 1. На заздалегідь визначені інформаційні позиції кодового слова помістимо k символів повідомлення.

Крок 2. Обчислимо за виразом (11) матрицю-рядок $\left\| S_j \right\|_r$.

Крок 3. Обчислимо за виразом (12) матрицю-рядок $\left\| c_i \right\|_r$.

Крок 4. Помістимо елементи матриці $\left\| c_i \right\|_r$ на перевірочні позиції кодового слова.

Несистематичний спосіб кодування полягає в наступному [13]. Несистематичне кодування алгоритмічно простіше, але його використання передбачає виділення інформаційної частини повідомлення на приймальній стороні з декодованого кодового слова, що вимагає додаткових обчислювальних витрат.

Скористаємося визначенням алгеброгеометричного коду через породну матрицю. Кодове слово у цьому випадку може бути сформоване за таким правилом:

$$c_i = \sum_{i \in I} I_j F_j(P_i), \quad i = \overline{0, n-1}$$

або в матричній формі як добуток інформаційного вектора-рядка на породну матрицю:

$$\left\| c_j \right\|_n = G \left\| I_i \right\|_k^T = \left\| F_i(P_j) \right\|_{n,k} \left\| I_i \right\|_k^T . \qquad (47)$$

Таким чином, для реалізації несистематичного способу кодування необхідно зберігати елементи матриці $\left\| F_i(P_j) \right\|_{n,k}$ або по черзі обчислювати їх як значення генераторних функцій у точках кривої.

Алгоритм несистематичного кодування задамо у вигляді послідовного формування символів кодового слова за правилом (47).

Розроблені алгоритми алгеброгеометричного кодування дозволяють формувати кодові слова для довільних k символів повідомлення. Алгоритми допускають реалізацію кодів по довільній кривій у P^2 над GF(q). Параметри таких кодів асимптотично лежать вище межі Варшамова-Гілберта.

Оцінимо алгоритмічну складність розроблених алгоритмів. Якщо заздалегідь сформовані $\left\| F_j(P_i) \right\|_{k,r}$ і $\left\| F_j(P_i) \right\|_{r,r}^{-1}$, то при систематичному кодуванні необхідно $k \times r$ операцій додавання і множення для обчислення вектора синдромів та $k \times r$ операцій додавання і множення для обчислення вектора перевірочних символів. Усього при відомих і збережених у пам'яті масивів $\left\| F_j(P_i) \right\|_{k,r}$ і $\left\| F_j(P_i) \right\|_{r,r}^{-1}$ необхідно виконати $r \times (k + r) = r \times n$ операцій додавання і множення. Формально, складність алгоритму систематичного кодування без урахування складності обчислення генераторних функцій дорівнює $O(r \times n)$.

Для несистематичного алгоритму кодування при відомих (заздалегідь сформованих) і збережених у пам'яті елементів $\left\| F_i(P_j) \right\|_{n,k}$ усього необхідно виконати $k \times n$ операцій додавання та множення. Формально складність алгоритму несистематичного ко-

дування без ураження складності обчислення генераторних функцій дорівнює $O(k \times n)$.

Таким чином, для алгеброгеометричних кодів з $R = k/n \sim 0{,}5$ обидва розроблені алгоритми мають еквівалентну алгоритмічну складність, порівняну з традиційними процедурами (складність алгоритмів циклічного кодування $O(k \times n)$).

Збереження елементів масивів $\left\|F_j(P_i)\right\|_{k,r}$ і $\left\|F_i(P_j)\right\|_{n,k}$ для довгих кодів може вимагати значних системотехнічних витрат. У цьому випадку доцільно по черзі обчислювати $F_i(P_j)$. Основною обчислювальною операцією в цьому випадку є знаходження значення генераторної функції F_i у точці алгебраїчної кривої P_j. У загальному вигляді для обчислення $F_i(P_j)$ у P^2 потрібно три операції піднесення до степеня і дві операції множення. Якщо прийняти рівними обчислювальну складність операцій множення і піднесення до степеня, то формально складність алгоритму систематичного кодування дорівнює $O(5 \times r \times n)$, складність алгоритму несистематичного кодування $O(5 \times k \times n)$.

Якщо при побудові генераторної матриці алгеброгеометричного коду використовувати тільки точки кривої вигляду $P(X, Y, 1)$, то треба спростити більш ніж на третину необхідні для алгеброгеометричного кодування обчислення. Так, для $F_i(P_j)$ у P^2 у цьому випадку потрібні дві операції піднесення до степеня та одна операція множення. Формально, у цьому випадку складність алгоритму систематичного кодування дорівнює $O(3 \times r \times n)$, складність алгоритму несистематичного кодування – $O(3 \times k \times n)$.

Таким чином, у результаті проведених досліджень розроблені методи і практичні алгоритми побудови алгеброгеометричних кодів, що дозволяють будувати кодові конструкції з необхідними конструктивними параметрами в систематичному і несистематичному вигляді, розробляти практичні схеми апаратної і програмної реалізації кодерів, складність яких порівняння з традиційними (наприклад, кодерами циклічних кодів).

6. Алгоритми декодування алгеброгеометричних кодів та їх підкодів. Розглянемо задачу декодування кодового слова алгеброгеометричного коду, а потім узагальнимо результат для обмежень кодів на довільне підполе.

Припустимо, що при передаванні по каналу з помилками кодове слово алгеброгеометричного коду спотворилося, вектор помилок позначимо як $e = (e_0, e_1, \ldots, e_{n-1})$. Прийняте слово c^* після передачі по каналу з помилками запишеться у вигляді $c^* = c + e = (e_0 + c_0, e_1 + c_1, \ldots, e_{n-1} + c_{n-1})$. Визначимо синдромну послідовність як вектор $S = (S_1, S_2, \ldots, S_r)$, обчислений за наступним правилом:

$$S_j = \sum_{i=0}^{n-1} c^* F_j(P_i), \quad j = 1, \ldots, r$$

або у матричній формі

$$\left\|S_j\right\|_r = \left\|F_j(P_i)\right\|_{n,r} \left\|c_i^*\right\|_n^T.$$

Очевидно, що

$$S_j = \sum_{i=0}^{n-1} \left[c_i F_j(P_i) + e_i F_j(P_i)\right] = \sum_{i=0}^{n-1} e_i F_j(P_i),$$

$$j = 1, \ldots, r$$

або в матричній формі

$$\left\|S_j\right\|_r = \left\|F_j(P_i)\right\|_{n,r} \left\|e_i\right\|_n^T = H \left\|e_i\right\|_n^T.$$

Значення синдрому залежить тільки від вектора помилок і не залежить від кодового слова.

Задача декодування алгеброгеометричного коду полягає у знаходженні вектора помилок $e = (e_0, e_1, \ldots, e_{n-1})$ за відомою синдромною послідовністю $S = (S_0, S_1, \ldots, S_{r-1})$.

Розглянемо як генераторні функції однорідні одночлени степеня degF. Кожен такий одночлен запишемо у вигляді

$$f_{lmp} = x^l y^m z^p, \; l + m + p = \deg F.$$

На множині проективних точок кривої X, які можуть бути представлені в однорідних координатах у вигляді $P(X, Y, 1)$, значення генераторних функцій наберуть вигляду $f_{lm} = X_i^l Y_i^m$, $i = 0, \ldots, n-1$, $l + m \le \deg F$. Перевірочна матриця H запишеться у вигляді

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ X_0 & X_1 & \ldots & X_{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ Y_0^{\deg F} & Y_1^{\deg F} & \ldots & Y_{n-1}^{\deg F} \end{pmatrix}.$$

Елементи синдромної послідовності, як елементи вектора $\left\|S_{lm}\right\|_r$, обчислимо за правилом

$$S_{lm} = \sum_{i=0}^{n-1} c_i^* X_i^l Y_i^m = \sum_{i=0}^{n-1} e_i X_i^l Y_i^m, \; l + m \le \deg F$$

або у матричній формі

$$\left\|S_{lm}\right\|_r = H \left\|c_n^*\right\|_n^T = \left\|X_i^l Y_i^m\right\|_{n,r} \left\|e_i\right\|_n^T. \qquad (48)$$

Таким чином, задача декодування алгеброгеометричного коду, побудованого через відображення проективних точок $P(X, Y, 1)$ кривої однорідними одночленами степеня degF, еквівалентна задачі розв′язання системи $r = d + g - 1$ нелінійних рівнянь від $3t$ змінних.

Для розв′язання цієї задачі скористаємося штучним прийомом, що полягає у введенні в розгляд многочлена локаторів помилок, розв′язання якого однозначно локалізують (указують місце розташування) виниклих помилок. Визначимо многочлен локаторів помилок алгеброгеометричного коду як многочлен від двох змінних, степеня (t – 1):

$$a_{00} + a_{10}x + \ldots + y^{t-1} = 0, \qquad (49)$$

де t – кількість помилок, що може виправити алгеброгеометричний код.

Помноживши обидві частини многочлена (49) на e_i і взявши суму за всіма i = 0, ..., n – 1 значеннями у точці ($x = X_i$, $y = Y_i$), одержимо рекурентний вираз

$$a_{00}S_{00} + a_{10}S_{10} + \ldots + S_{0\,t-1} = 0,$$

який задає систему лінійних рівнянь щодо невідомих коефіцієнтів многочлена локаторів помилок. У матричному вигляді система лінійних рівнянь запишеться у вигляді

$$\begin{pmatrix} S_{00} & S_{10} & \ldots & S_{1\,t-2} \\ S_{10} & S_{20} & \ldots & S_{2\,t-2} \\ \ldots & \ldots & \ldots & \ldots \\ S_{1\,t-2} & S_{0\,t-2} & \ldots & S_{2\,2t-4} \end{pmatrix} \times$$

$$\times \begin{pmatrix} a_{00} \\ a_{10} \\ \ldots \\ a_{1\,t-2} \end{pmatrix} = \begin{pmatrix} -S_{0\,t-1} \\ -S_{1\,t-1} \\ \ldots \\ -S_{1\,2t-3} \end{pmatrix}. \qquad (50)$$

Після знаходження коефіцієнтів многочлена локаторів помилок процедура локалізації помилок полягає в підстановці всіх можливих локаторів і виборі тих з них, що перетворюють у нуль многочлен локаторів помилок, тобто підставляються усі пари (X, Y), що ототожнюють, усі проективні точки кривої, задані в однорідних координатах P(X, Y, 1).

Після знаходження локаторів помилок, що вказують на розташування виниклої помилки, процедура знаходження кратності помилки (значення всіх $e_i \neq 0$) полягає в підстановці локаторів у систему (48), яка вироджується в систему до r лінійних рівнянь відносно до t невідомих.

Алгоритм декодування алгеброгеометричних кодів задамо у вигляді послідовності наступних кроків.

Крок 1. За виразом (48) обчислимо елементи синдромної послідовності.

Крок 2. Розв′яжемо систему лінійних рівнянь (50). Одержимо коефіцієнти многочлена локаторів помилок.

Крок 3. Підставимо всі пари (X, Y), що відповідають проективним точкам кривої, у многочлен локаторів помилок. Ті пари, що при підстановці в цей многочлен перетворюють його на нуль, локалізують помилки, тобто вказують на їх шукане розташування.

Крок 4. Підставляємо отримані локатори помилок у систему рівнянь (48). Розв′язання системи лінійних рівнянь дасть значення (кратність) помилок, що відбулися. Локалізація помилок і знайдені їх значення дозволяють сформувати вектор помилок $e = (e_0, e_1, \ldots, e_{n-1})$.

Крок 5. Виправимо помилки: $c = c^* - e$.

Основні етапи розробленого алгебраїчного алгоритму складаються в розв′язанні системи лінійних рівнянь (кроки 2 і 4) і виконанні кроку 3. Ці стандартні процедури, а також процедура обчислення вектора синдромів можуть бути реалізовані кожним з відомих на сьогоднішній день алгоритмів [2 – 6]. Складність розв′язання системи лінійних рівнянь методом Гаусса – $O(n^2)$, де n – кількість змінних. При розв′язанні системи лінійних рівнянь (50) оцінимо кількість змінних.

Многочлен локаторів помилок (49) заданий як многочлен від двох невідомих і складається з усіх одночленів від двох змінних степеня (t – 1). Кількість одночленів від двох змінних степеня b визначимо з виразу

$$M = C_{b-1}^{1} = b - 1.$$

Тоді кількість невідомих у многочлені локаторів помилок (49) запишеться у вигляді

$$n = \sum_{i=1}^{t-1} C_{i-1}^{1} = \sum_{i=1}^{t-1} (i-1) = \frac{t^2 - t}{2}.$$

Отже, для декодування алгеброгеометричного коду, побудованого через відображення проективних точок P(X, Y, 1), на кроці 2 необхідно розв′язати систему лінійних рівнянь від $(t^2 - t)/2$ змінних, складність її розв′язання методом Гаусса – $O((t^2 - t)^{2/4})$. Загальна складність алгоритму декодування – $O(4t^2 + (t^2 - t)^{2/4})$.

Таким чином, у результаті проведених досліджень розроблені методи і практичні алгоритми алгебраїчного декодування алгеброгеометричних кодів, що дозволяють звести задачу локалізації і виправлення помилок до розв′язання систем лінійних рівнянь. Це дозволяє використовувати прості схеми апаратної і програмної реалізації, складність яких зростає поліноміально зі зростанням відправляючого коду здатності. У [15 – 16] досліджені неалгебраїчні методи і практичні алгоритми неалгебраїчного декодування алгеброгеометричних кодів, які дозволяють використовувати мажоритарні і переставні

процедури неалгебраїчного декодування недвійкових нециклічних блокових кодів, що дозволяє у деяких випадках без використання складних алгебраїчних перетворень реалізувати прості схеми декодування.

Висновки

1. На основі теорії інформації, теорії чисел і алгебраїчної теорії блокових кодів розроблена єдина методологія побудови найбільш важливих класів алгебраїчних блокових кодів через обмеження лінійних блокових кодів виникаючих на алгебраїчних кривих (алгеброгеометричних кодів). Це дозволяє на відміну від відомих підходів, використовуючи єдині методологічні принципи, досліджувати структуру, логічну організацію методів і засобів побудови важливих класів алгебраїчних блокових кодів, одержати цілісне уявлення про закономірності їх синтезу та істотних зв'язків.

2. Розроблено математичний апарат побудови лінійних блокових кодів через обмеження алгеброгеометричних кодів на довільне підполе, який відрізняється від відомих наявністю загальних системно-концептуальних ознак у теорії побудови великих класів блокових кодів, що дозволяє узагальнити в єдину методику відомі методи синтезу кодів, алгоритми кодування і декодування.

3. Розроблені методи і практичні алгоритми побудови алгеброгеометричних кодів, які дозволяють будувати кодові конструкції з необхідними параметрами в систематичному і несистематичному вигляді; розроблені методи і практичні алгоритми алгебраїчного декодування алгеброгеометричних кодів, які дозволяють звести задачу локалізації і виправлення помилок до розв′язання систем лінійних рівнянь.

СПИСОК ЛІТЕРАТУРИ

1. Шеннон К. Связь при наличии шума // Теория информации и ее приложения: Сб. переводов. – М.: ФИЗМАТГИЗ. – 1959. – С. 82 – 112.

2. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.

3. Берлекэмп Э.Р. Алгебраическая теория кодирования: Пер. с англ. – М.: Мир, 1971. – 477 с.

4. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с.

5. Кларк Дж.-мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи. – М.: Радио и связь, 1987. – 392 с.

6. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. – М.: Мир. – 1978. – 576 с.

7. Гоппа В.Д. Коди на алгебраических кривих // Докл. АН СССР. – 1981. – Т. 259, № 6. – С. 1289 – 1290.

8. Гоппа В.Д. Коди и информация // Успехи математических наук. – 1984. – Т. 30, вип. 1 (235). – С. 77 – 120.

9. Влэдуц С. Г., Манин Ю. И. Линейние коди и модулярние кривие // Современные проблемы математики. – М.: ВИНИТИ. – 1984. – Т. 25. – С. 209 – 257.

10. Voss, Tom Hoholdt. An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zink bound. The first steps // IEEE Trans. Info. Theory. – 1997. – Vol. IT-43. – P. 128 – 135.

11. Ruud Pellikaan. Asymptotically good sequences of curves and codes // Proc. 34th Allerton Conf. on Communication, Control and Computing. – Urbana-Champaign. – 2 – 4 October, 1996. – P. – 276 – 285.

12. Кузнецов А.А. Энергетическая эффективность алгеброгеометрических кодов // Электронное моделирование: Международний научно-теоретический журнал. – К: НАНУ, РАН. – 2004. – № 2. – С. 27 – 38.

13. Кузнецов А.А., Северинов А.В., Лысенко В.Н., Науменко И.В. Алгоритм помехоустойчивого кодирования с использованием кодов по кривим Эрмита // Системи обробки інформації: Зб. наук. пр. – Х.: ХВУ. – 2003. – Вип. 6(28). – С – 181 – 185.

14. Кузнецов А.А., Северинов А.В., Задворний Д.А. Лысенко В.Н. Алгебраическое декодирование кодов по кривим Эрмита // Вісник НТУ «ХПІ». – Х.: НТУ "ХПІ". – 2003. – № 26. – С. 95 – 102.

15. Кузнецов А.А., Северинов А.В., Лисенко В.Н. Алгоритм мажоритарного декодирования алгеброгеометрических кодов // Системи обробки інформації: Зб. наук. пр. – Х.: НАНУ, ПАНМ, ХВУ. – 2003. – Вип. 4 (26). – С. 61 – 66.

16. Северинов А.В., Кузнецов А.А., Куриш В.В. Разработка алгоритма декодирования аггеброгеометрических кодов // Системи обробки інформації: Зб. наук. пр. – Х.: НАНУ, ПАНМ, ХВУ. – 2002. – Вип. 1 (17). – С. 161 – 163.

Надійшла 27.09.2005

Рецензент: д-р фіз.-мат. наук професор С.В. Смеляков, Харківський університет Повітряних Сил.