УДК 025.7/9
© Ю. Наконечний[1], П. Гаранюк[1], Я. Кавин[2], 2012

ЗАХИСТ БЛАНКІВ ЦІННИХ ПАПЕРІВ МЕТОДОМ КОМБІНАТОРНОЇ ОПТИМІЗАЦІЇ

Дослідження моделей і методів комбінаторної оптимізації з застосуванням монолітних кодів в задачах інформаційної техніки і проектування систем кодування та перетворення сигналів.

The research of the models and methods of combinatorics optimization with monolithic codes using in the tasks of informative engineering and the planning of the systems encryption and signals transformation.

1. ВСТУП

Під монолітним розуміємо код, дозволені комбінації якого складаються з пакетів однойменних символів, що знаходяться один поруч одного.

Монолітний двійковий код має ряд переваг перед іншими кодами. Одна з них – простота виявлення та виправлення помилок на приймальній стороні, бо поява хоча б одного символу "1" серед нулів, або символу "0" серед одиниць у прийнятій кодовій комбінації вказує на помилку. Помилка не виявляється лише у тих випадках, коли хибний сигнал виникає в першому або останньому символах пакету. Якщо в монолітному коді з'являються хибні символи, то всі вони або частина з них зразу ж виявляються, що спрощує виявлення помилок і забезпечує високу завадостійкість монолітного коду.

Досліджуючи системи кодування інформації з різними законами розподілу ваг розрядів монолітного коду, легко побачити, що в деяких випадках розподілу ваг монолітний код виявляється надміру надлишковим, бо одні й ті ж числа подаються кількома різними кодовими комбінаціями двійкового позиційного коду.

2. ПОСТАНОВКА ПРОБЛЕМИ

Розв'язок поставленої задачі зводяться до пошуку оптимального комбінаторного варіанту ваг розрядів монолітного коду, при якому будь–яке натуральне число можна було б подати в монолітному коді єдино можливим способом.

[1] Національний університет «Львівська політехніка»
[2] Українська академія друкарства

Виникає проблема вибору оптимальної системи ваг розрядів, суть якої полягає в тому, щоб множині кодових комбінацій монолітного коду взаємно однозначно відповідала множина чисел натурального ряду.

Інтерес для дослідження становлять системи кодування, які базуються на застосуванні комбінаторних властивостей ідеальних кільцевих в'язанок [4]. Проста ідеальна кільцева в'язанка (ІКВ) – це алгебраїчна структура, утворена на послідовності цілих додатних чисел, значення яких, як і значення сум поруч розміщених між собою чисел, вичерпують натуральний ряд. Елементи ІКВ розміщені один біля одного у вигляді кільця.

Нижче наведена таблиця кодових комбінацій, утворених на простій ІКВ шостого (n=6) порядку (1,3,2,7,8,10):

Таблиця 1

Кодові комбінації кільцевого монолітного коду (1,3,2,7,8,10).

Число	Код	Число	Код
	000000		111001
	100000		001110
	001000		000011
	010000		100011
	110000		011110
	011000		111110
	111000		110011
	000100		111101
	000010		111011
	001100		000111
	000001		100111
	100001		001111
	011100		101111
	111100		110111
	110001		011111
	000110		111111

Потужність КМК, реалізованого на ІКВ n–го порядку, визначається загальним числом способів утворення кодових слів:

$$N^{(K)}=n(n-1)+1. \quad (1)$$

Завадостійкість монолітного коду можна оцінити за співвідношенням кількості помилкових кодових комбінацій, які виявляються $M_{виявл.}$ (або виправляються $M_{випр.}$), до загальної кількості усіх можливих комбінацій заданої розрядності. Нехай n – розрядність кодового слова, а r – число помилкових символів у кодовому слові. Ефективність КМК щодо можливості виявлення і виправлення помилок можна оцінити за допомогою наступних залежностей:

$$\text{Ì}^{(k)}_{\text{‰□Ø‰‘.}} = \frac{C_{n-4}^{r}}{C_{n}^{r}}100\%, r < n-4 \quad (2)$$

$$\text{Ì}^{(k)}_{\text{‰□•ð.}} = \frac{C_{n-8}^{r}}{C_{n}^{r}}100\%, r < n-8\,. \quad (3)$$

Алгоритм побудови кільця монолітного коду складається з наступних кроків:

Крок 1. За значеннями N і R обчислюється оцінка найбільшого граничного значення L_{max} суми ЧЛВ при $R=1$ за формулами [4] і оцінка найбільшого значення суми ЧЛВ відносно суми ЧКВ L_{max} за формулами [4];

Крок 2. Заготовлюється масив із N комірок, пронумерованих у зростаючому порядку;

Крок 3. В перші R комірок масиву записується число, з якого починається відлік в ЧЛВ, в $(R+1)$ –у – наступне, в решту заносяться нулі;

Крок 4. Перший раз число A визначається як збільшене на одиницю найбільше число найкоротшого ряду послідовності чисел, утвореного на множині сум, які знайдені на всіх окремих послідовностях, що належать масиву. Наступний раз число A з тим самим значенням визначається як збільшене на одиницю наступне за найбільшим числом найкоротшого ряду послідовності чисел, поки сума усіх чисел масиву L_N^R менша за L_{max} При існуючих вільних комірках масиву число A записується у вільну комірку з найменшим порядковим номером і обчислюється нове значення суми L_N^R усіх чисел масиву; у випадку коли $L_N^R \le L_{max}$ виконується крок 5, а при $L_N^R > L_{max}$ – виконується крок 7;

Крок 5. Обчислюється нове значення суми елементів масиву ЧЛВ L_{max} . При існуючих у масиві вільних комірках знаходяться всі суми на всіх послідовностях, а при їх відсутності – всі лінійні сумі на єдиній послідовності:

а) якщо кожна зі знайдених сум зустрічається не більше R разів і є вільні комірки, то здійснюється перехід до кроку 4. При відсутності вільних комірок і при виконанні умови, що нове значення суми L_N^R не більше попереднього, отримується варіант ЧЛВ, після чого виконується крок 7. В іншому випадку виконується крок 6;

б) якщо хоча б одна зі знайдених сум з'являється більше R разів, то виконується крок 6;

Крок 6. Знаходиться найбільше число B, потім визначається чи є вільний номер комірки з номером більшим ніж той, де розташоване число B; якщо така комірка існує, то з комірки з меншим номером число B переноситься у вільну комірку з більшим номером, після чого виконується крок 5; в протилежному випадку виконується крок 7.

Крок 7. Звільняється комірка з числом B і виконується крок 6. Ознакою закінчення обчислень при побудові повної сім'ї ЧЛВ служить поява числа, з якого починається відлік в ЧЛВ в комірці $\frac{N+3}{2}$ при умові його відсутності в попередніх комірках для непарних значень N і аналогічно в комірці $\frac{N+2}{2}$ для парних значень N .

Для побудови циклічного коду за допомогою ІКВ виділимо рядок із S_n пронумерованих у зростаючому порядку клітинок одновимірного масиву і заповнимо інформаційними "одиницями" клітинки, номери яких збігаються з числами, визначеними з ІКВ. У клітинки, що залишилися незаповненими, занесемо "нулі". Утворена послідовність одиниць і нулів є S_n–розрядною кодовою комбінацією, циклічним зсувом якої можна одержати й решта дозволених комбінацій.

Кожна з $S_n(S_n–1)/2$ різних пар кодових комбінацій містить точно R із n одиничних символів в однойменних розрядах, що випливає з властивостей ІКВ. Решта n–R символів однієї і стільки ж іншої кодової комбінації відрізняються від символів, що містяться в однойменних розрядах. Тому мінімальна кодова відстань для даного коду визначається як:

$$d_{min}=2(n–R). \qquad (4)$$

Число помилок, які можна виявити t_1, і число помилок, що можна виправити t_2 за допомогою коректуючого коду, визначається мінімальною кодовою відстанню залежностями:

$$t_1 \le d_{min} - 1,\ t_2 \le (t_1 - 1)/2. \quad (5)$$

Формули для визначення кількості помилок, які можуть бути виправлені t_2 або виявлені t_1:

$$t_1 \le 2(n - R) - 1,\ t_2 \le n - R - 1. \quad (6)$$

Потужність побудованого за допомогою ІКВ коду можна збільшити вдвічі, якщо складену вище таблицю доповнити комбінаціями, які утворюються зі знайденої таблиці шляхом заміни інформаційних одиниць нулями, і навпаки.

Кодова відстань знаходиться як

$$d_{1,2} = S_n - 2(n - R) \quad (7)$$

Формули для визначення числа помилок, які підлягають виявленню чи виправленню за допомогою описаного коду:

$$\left.\begin{aligned} t_1 &\le 2(n - R) - 1 \\ t_2 &\le n - R - 1 \end{aligned}\right\}, \text{ якщо } S_n \ge 4(n - R); \quad (8)$$

$$\left.\begin{aligned} t_1 &\le S_n - 2(n - R) - 1 \\ t_2 &\le \frac{S_n - 2(n - R + 1)}{2} \end{aligned}\right\}, \text{ якщо } S_n < 4(n - R); \quad (9)$$

У розглянутих випадках значення параметрів n і R не зв'язані між собою будь–якою залежністю і можуть вибиратися довільно. При цьому виникає питання про встановлення оптимального співвідношення між n і R, за дотримання якого розглянутий код набуває додаткових переваг. Завадостійкість коду зростає зі збільшенням різниці $\delta = n - R$.

Максимальне значення δ досягається за умови:

$$S_n = 2n. \quad (10)$$

Співвідношення між параметрами n і R, коли код набуває здатності виявляти та виправляти максимально можливу кількість помилок:

$$\mathrm{P} = \begin{cases} n/2, n - napíe \\ (n-1)/2, n - íenapíe \end{cases} \qquad (11)$$

Побудовані за допомогою ІКВ завадостійкі коди дають змогу виявляти до n–1 або виправляти до n/2–1 помилок для парних, і виявляти до n або виправляти до (n–1)/2 помилок для непарних значень n.

3. ДОСЛІДЖЕННЯ АЛГЕБРАЇЧНИХ МОДЕЛЕЙ КОДІВ З КІЛЬЦЕВОЮ СТРУКТУРОЮ

Різноманітність алгебричних моделей монолітного коду при існуючій многовидності їх інтерпретацій через циклічні блок–схеми, різницеві множини, скінченні афінні та проективні площини, матриці Адамара [1] та інші комбінаторні об'єкти вимагають розробки єдиного підходу до методів синтезу згаданих числових моделей. Один із таких підходів базується на використанні для побудови коду властивостей полів Галуа та геометрій над ними. Тому доцільно нагадати основні означення та деякі властивості полів Галуа [2].

Математичні моделі ідеальних монолітних кодів з кільцевою структурою це такі моделі, які дозволяють кодувати числа так, що будь–яке число від 0 до *W* (де *W* – сума значень ваг усіх розрядних цифр цього коду) можна представити двійковим монолітом точно N+1 різними способами, де N+1 – кратність способів кодування. Неідеальні моделі за своїми комбінаторними властивостями можуть бути близькими до ідеальних, але з тих чи інших причин не задовольняють усім вимогам, які ставляться до ідеальних моделей.

Для всякого степеня простого числа *p* і будь–якого $n \geq 1$ існує єдине з точністю до ізоморфізму $GF(p^n)$, тобто поле зі скінченним числом елементів або просто поле Галуа, де *GF* означає Galois Field.

Поле $GF(p^n)$ можна зобразити як множину всіх класів лишків за модулем довільного полінома *f(x)* степеня *n* незвідного над полем *GF(p)*. Поліном *f(x)* степеня $n \geq 1$ з коефіцієнтами із поля *GF(p)* є незвідним над полем *GF(p)*, якщо його не можна записати у вигляді $f(x) = A(x) \cdot B(x)$, де *A(x)* і *B(x)* поліноми над *GF(p)*. Наприклад, незвідним поліномом у полі *GF(3)* буде поліном $f = x^2 - 2$. В цьому досить легко переконатися, перевіривши що він не ділиться без залишку на поліноми степеня *n-1* з коефіцієнтами із поля *GF(3)*, тобто на

поліноми $x, x-1, x-2$. Поліном *f(x)* степеня $n \geq 1$ незвідний над полем *GF(q)*називається первісним, якщо його корінь θ є первісним елементом поля $GF(q^s)$. Якщо $s=1, \quad q=p^n$, то первісним буде такий незвідний над полем $GF(p^n)$ поліном степеня *n*, корінь якого в полі $GF(p^n)$ має період p^n-1.

У цьому випадку всі корені полінома *f(x)* первісні. Кожен відмінний від нуля елемент *k* поля *GF(q)* представляється у виді

$$k=\theta^t \tag{12}$$

Характеристична функція

$$F_t(x)=f(x;\theta^t) \tag{13}$$

елемента θ^t є поліномом степеня *n* з коефіцієнтами з *GF(q)*. Якщо $F_t(\theta^t)$ має степінь m над *GF(q)*, то $n=mr$ і $f_t(x)=[g_t(x)]r$, де $g_t(x)$– мінімальна функція над *GF(q)* елемента θ^t і її степінь дорівнює *m*.

У полі $GF(q^s)$ всі його q^s-1 ненульові елементи різні та утворюють циклічну групу за операцією множення.

Відомо, що первісний елемент *x* поля $GF(q^s)$ має максимально можливий період q^s-1 елементів цього поля, а степені x^κ (к=0, 1,..., p^s-2) перебігають усі ненульові елементи $GF(q^s)$ і є також елементами цього поля [2]. Оскільки $x^{p^s-1} \equiv 1$, то $x^{p^s}=x, x^{p^s+1} \equiv x^2$ і т.д. Отже, мультиплікативна група (група за операцією множення) $GF(q^s)$ є циклічною. Якщо деякий елемент *x* поля $GF(q^s)$ має період q^s-1 і є коренем полінома *f(x)*, то єдиними коренями полінома *f(x)* будуть також і елементи поля $x^2, x^3, ..., x^{q^s-2}$.

Автоморфізми поля $GF(q^s)$ утворюють циклічну групу порядку *S*, яка породжується автоморфізмом $\alpha: \quad x \to x^p$ для будь–якого $x \in GF(q^s)$. Іншими словами, це така взаємна відповідність, при якій корені даного незвідного полінома переводяться в інші корені цього ж полінома. В цьому можна переконатися, побудувавши поля для різних коренів полінома. Так корені полінома $f(x)=x^2+x+2$ є перві-

сними елементами поля $GF(3^2)$. Якщо коренем полінома візьмемо x, то отримаємо поле $GF_1(3^2)$, елементами якого за модулем $q=3$ будуть:

$$x^0 \equiv 1$$
$$x^1 \equiv x$$
$$x^2 \equiv 2x + 1$$
$$x^3 \equiv 2x + 2$$
$$x^4 \equiv 2$$
$$x^5 \equiv x$$
$$x^6 \equiv x + 2$$
$$x^7 \equiv x + 1$$

Якщо коренем незвідного полінома візьмемо $x^{3=}2x+2$, то отримаємо поле $GF_2(3^2)$, елементами якого будуть:

$$x^0 \equiv 1$$
$$x^1 \equiv 2x + 2$$
$$x^2 \equiv x + 2$$
$$x^3 \equiv x$$
$$x^4 \equiv 2$$
$$x^5 \equiv x + 1$$
$$x^6 \equiv 2x + 1$$
$$x^7 \equiv 2x$$

Елементи поля $GF_1(3^2)$ взаємно однозначно відображаються в елементи $GF_2(3^2)$, причому задовольняються всі закони поля [1,2].

Підполя поля $GF(p^n)$ – це поля $GF(p^m)$, де m ділить n. Для будь–якого n поле $GF(p^n)$ має єдине підполе $GF(p^m)$, що складається з елементів поля $GF(p^n)$, які задовольняють рівняння $z^{p^m} = z$. Первісний

елемент *x* поля $GF(p^n)$ задовольняє рівняння $g(x)=0$, де $g(x)$ – незвідний над $GF(p^m)$ поліном степеня n/*m*.

Наприклад, поле $GF(5^2)$ можна подати класами лишків за модулем $f(x)$, де $f(x)$ – незвідний над $GF(5^2)$ поліном степеня 2. Такими незвідними поліномами є $f_1 = x^2 - 2$ та $f_2 = x^2 + x + 1$. Тому утворюються два ізоморфні поля F_1 та F_2 з 25 елементами.

Поліном $f(x) = x^6 + x^5 + x^3 + x^2 + 1$ незвідний над $GF(2)$. Отже, лишки $A(x)\ (mod\ f(x))$ утворюють поле $GF(2^6)$ з 64 елементами. Первісним елементом в цьому полі є елемент *x*, а його степені дають ненульові елементи поля $GF(2^6)$: $1, x, x^2, ..., x^{62}$. Підполе $GF(2)$ поля $GF(2^6)$ містить елементи 0, 1; $GF(2^2)$ – елементами $0,1,x^{21},x^{42}$ що задовольняють рівняння $z^4 = z$; $GF(2^3)$ – елементами $0,1, x^9, x^{18}, x^{27}, x^{36}, x^{45}, x^{54}$, де $z^8 = z$. Автоморфізми поля $GF(2^6)$ утворюють циклічну групу порядку 6, яка породжується автоморфізмом $\alpha : z \to z^2 = (z)\alpha$ для будь–якого $z \in GF(2^6)$.

Простір всіх векторів $(a_0, a_1, ..., a_s)$, $a_i \in F$, де *F*– довільне поле є проективною геометрією $PG(s, F)$ розмірності *S* над полем *F*, а підпростір розмірності *s-1* називається гіперплощиною.

У полі $GF(q), q = p^r$ існує q^{s+1} векторів $(x_0, ..., x_s)$, $x_i \in GF(q)$ таких, що кожен з q^{s+1}-1 ненульових векторів визначає одну з $(q^{s-1} - 1)/(q - 1)$ різних точок, і така ж кількість гіперплощин, причому кожна гіперплощина має $(q^{s-1} - 1)/(q - 1)$ різних точок, а утворений на спільних для двох різних гіперплощин підпростір розмірності *n-2* містить $(q^{s-1} - 1)/(q - 1)$ точок.

(Теорема Зінгера) Гіперплощини геометрії $PG(s, q), q = p^r$, які розглядаються як блоки, і точки як елементи, утворюють симетричну блок–схему з параметрами v, k, λ. Для зінгерових різницевих множин між параметрами $W_n = v,\ \ k = n,\ \ N = \lambda - 1$, (де Wn – потужність кільцевого монолітного коду, n– кількість розрядів кодових слів, N– число кодових слів з однаковими сумами ваг розрядів) існує зв'язок [1]:

$$v = \frac{q^{s+1} - 1}{q - 1}, \qquad k = \frac{q^s - 1}{q - 1}, \qquad \lambda = \frac{q^{s-1} - 1}{q - 1} \tag{14}$$

де $q = p^{\alpha}$ – степінь простого числа, $s\rangle 0$.

На підставі (2.3) можна визначити

$$\alpha = \log_p \frac{n-1}{N+1}$$

та

$$s = \log_{\frac{n-1}{N+1}} \left(n - (N+1)\right) + 1$$

Із цих залежностей легко визначити степінь полінома, з допомогою якого будується алгебрична модель ІКМК.

Для симетричної блок–схеми виконується співвідношення:

$$k(k-1) = \lambda(v-1) \qquad (15)$$

При $\lambda = 1$ симетрична блок–схема буде називатися скінченною проективною площиною порядку *k-1*.

Оскільки симетрична блок–схема є циклічною, а точки у будь–якій гіперплощині визначають (v, k, λ) – різницеву множину [3], то ідеальну кільцеву в'язанку порядку n>2 можна розглядати як скінченне поле, в якому є $n-1 = p^{\alpha}$ елементів, що відповідає певній циклічній блок–схемі та різницевій множині.

Для побудови алгебричної моделі монолітного коду з параметрами Wn= v+1, n=k, N=λ–1, необхідно обрати або обчислити деякий незвідний над полем $GF(p^s)$ поліном, визначити первісний елемент *x* цього поля з максимально можливим періодом згаданого елемента і обчислити усі його степені x0, x1,…, xz, (z=qs–2), які повинні "пробігати" усі значення ненульових елементів $GF(p^s)$. Далі слід дослідити побудовану алгебричну структуру з метою визначення значень вагових розрядів усіх дозволених кодових комбінацій монолітного коду. Важливо також дослідити можливості побудови різних варіантів (інваріантів) розподілу значень вагових розрядів монолітних кодів з однаковими параметрами, що ускладнюється із–за необхідності урахування різних полів, для яких різні поліноми відповідають побудові кодів з однаковими параметрами. Так, наприклад, побудувавши алгебричні моделі за двома первісними поліномами в полі *GF(3)*:

$f_1(x) \equiv x^3 - x^2 - 2$	$f_2(x) \equiv x^3 - 2x^2 - 1$
$x \equiv x$	$x \equiv x$
$x^2 \equiv x^2$	$x^2 \equiv x^2$
$x^3 \equiv x^2 + 2$	$x^3 \equiv 2x^2 + 1$
$x^4 \equiv x^2 + 2x + 2$	$x^4 \equiv x^2 + x + 2$
$x^5 \equiv 2x + 2$	$x^5 \equiv 2x + 1$
$x^6 \equiv 2x^2 + 2x$	$x^6 \equiv 2x^2 + x$
$x^7 \equiv x^2 + 1$	$x^7 \equiv 2x^2 + 2$
$x^8 \equiv x^2 + x + 2$	$x^8 = x^2 + 2x + 2$
$x^9 \equiv 2x^2 + 2x + 2$	$x^9 \equiv x^2 + 2x + 1$
$x^{10} \equiv x^2 + 2x + 1$	$x^{10} \equiv x^2 + x + 1$
$x^{11} \equiv x + 2$	$x^{11} \equiv x + 1$
$x^{12} \equiv x^2 + 2x$	$x^{12} \equiv x^2 + x$
$x^{13} \equiv 2$	$x^{13} \equiv 1$

Ми бачимо, що ці моделі відповідають одному з варіантів монолітного коду із заданими параметрами, а саме $n = 4$, $N = 0$, $W_n = 13$. Тому, на жаль, не завжди вдається підібрати відповідні моделі для швидкої побудови монолітних кодів з відповідними параметрами. Питання побудови повних сімей таких кодів ускладнюється ще й тим, що існує нескінченно багато випадків нееквівалентних алгебричних моделей, тобто таких, які не можна утворити одна з одної методами алгебричних перетворень.

4. ВИСНОВКИ

Показана можливість спрощеної побудови за допомогою ІКВ моделей монолітного коду розширеного класу завадостійких кодів, створення ефективних алгоритмів кодування і декодування інформації й ряду інших задач.

Дослідження моделей і методів комбінаторної оптимізації розширює сферу практичних застосувань монолітних кодів в задачах інфор-

маційної техніки і проектування систем кодування та перетворення сигналів.

Запропонований алгоритм забезпечує захист архівованих зображень цінних паперів від несанкціонованого доступу, завдяки їх проміжному перетворенню в ІКВ–код, параметри і система порозрядного відліку якого відомі лише користувачеві.

1. Холл М. Блок–схемы. // Прикладная комбинаторная математика. М., 1968. 2. Різник В.В., Кісь Я.П. Завадостійкі коди на ідеальних кільцевих в'язанках. //Вимірювальна техніка і метрологія. – Вісник Державного університету "Львівська політехніка" N51., м.Львів, 1995 р. с.22–23. 3. Різник О.Я. Завадостійкий спосіб перетворення сигналів // Матеріали Четвертої укр. конф. з автоматичного керування ("Автоматика–97"). – Черкаси. – 1997. – С.34. 4. Різник В.В., Різник О.Я. Оцінка нижнього граничного значення довжини числових лінійок–в'язанок //Волинський математичний вісник. –Рівне. – 1997. – Вип.4. – С.131–134. 5. Gao Shuhong, Howell Jason, Panario Daniel. Irreducible polynomials of given forms. Finite Fields: Theory, Applications, and algorithms: Fourth International Conferense on Finite Fields: Theory, Applications, and algorithms, Waterloo, Aug. 12–15,1997. Providense (R.I): Amer.Math.Soc.1999, p.43–54. 6. Wan Dading. Generators and irreducible polynomials over finite fields. Math. Comput.1997. 66 №219,pp.1195–1212. 7. Wei Shimin, Xiao Guozhen, Chen Zhong. A fast algorithm for determinating the minimal polynomial of a sequence with period $2p^n$ over GF(q). IEEE. Trans.Inf.Theory.– 2002.48, №10, pp.2754–2758.