Висновок

Алгоритм забезпечує захист даних від несанкціонованого доступу завдяки їхньому проміжному перетворенню на код в'язанки, параметри якої відомі тільки користувачу. За допомогою монолітних кодів, побудованих за допомогою в'язанок, можна застосовувати ефективні алгоритми кодування і декодування інформації, що розширяє сферу практичних застосувань у задачах інформаційної техніки і проектування систем кодування [6, 7].

Результати досліджень кодування інформації на основі числових в'язанок дають підстави стверджувати про можливості їхнього використання у сучасних інформаційних технологіях для задач захисту інформації [1, 5].

1. Дурняк Б.В., Різник О.Я., Різник В.В., Я.П. Кісь Я.П., Парубчак В.О.. Захист даних методом комбінаторної оптимізації // Праці третьої міжнародної наукової конференції ISDMIT'2007, м.Євпаторія. т.2, с.152–153. 2. Ризныk О.Я. Комбинаторные модели для синтеза технических устройств и систем на основе числовых линейных сцепок // Контрольно-измерительная техника. – Львов: Вища школа. – 1989. – Вып.45. – С.23–25. 3. Різник В.В. Синтез оптимальних комбінаторних систем. – Львів, 1989. 4. Різник О.Я. Завадостійкий спосіб перетворення сигналів // Матеріали Четвертої укр. конф. з автоматичного керування ("Автоматика-97"). – Черкаси. – 1997. – С.34. 5. Різник О.Я., Парубчак В.О., Скрибайло-Леськів Д.Ю. Використання числових в'язанок для кодування інформації // Праці міжнародної конференції "Сучасні комп'ютерні системи та мережі: розробка та використання" (ACSN'2007). С.112–114. 6. Різник О.Я., Парубчак В.О., Скрибайло-Леськів Д.Ю. Кодування інформації за допомогою монолітного коду. Праці 2-ї міжнародної науково-практичної конференції "Інформаційні технології в наукових дослідженнях і навчальному процесі", м. Луганськ, 2007, т.2. С.88–92. 7. Різник О.Я., Стасевич С.П., Парубчак В.О., Скрибайло-Леськів Д.Ю. Швидкий синтез подібних кодів Баркера // Праці міжнародної конференції з математичного моделювання AMSE'2007, м. Алушта. – С. 23–24.

УДК 004.421

О.В. Бандирська[1], В.В. Різник[2], І.Ю. Юрчак[3]
Національний університет "Львівська політехніка",
[1]кафедра інформаційно-вимірювальних технологій,
[2]кафедра автоматизованих систем управління,
[3]кафедра систем автоматизованого проектування

АЛГЕБРИЧНИЙ МЕТОД ПРОЕКТУВАННЯ КРУГОВИХ ШКАЛ З ВИСОКОЮ РОЗДІЛЬНОЮ ЗДАТНІСТЮ

Розглядається алгебричний метод проектування нееквідистантних кругових шкал з підвищеною роздільною здатністю. Ці шкали ґрунтуються на так званих "ідеальних кільцевих в'язанках". Використовується принцип "оптимальних структурних пропорцій".

Algebraic method for design of non-uniform ring scales with improved resolving ability is described. These scales has been based on the so-called "Gold Ring Bundles". The principle of the "optimum structural proportions" (OSP) is applicated.

Алгебричні моделі та методи проектування систем будь-якого призначення широко застосовуються в радіоелектроніці, технічній кібернетиці, інформаційно-вимірювальній та обчислювальній техніці, а комбінаторні конфігурації широко використовуються для оптимального

проектування багатьох пристроїв мікро- і наноелектроніки. Актуальними є дослідження властивостей наявних і пошук нових комбінаторних моделей, які дають змогу швидко знаходити способи побудови систем та виявляти теоретичні зв'язки з класичними математичними методами оптимального просторового розміщення структурних елементів систем.

Аналіз проблеми та постановка задачі

Для проектування синтезу систем застосовують здебільшого класичні методи комбінаторного аналізу, що ґрунтуються на положеннях комбінаторного аналізу з використанням табличних, теоретико-числових та матричних інтерпретацій, методи апарата скінченних груп перестановок, теорії чисел, схеми відношень, а також методи, пов'язані з використанням апарату теорії полів [1].

Метод побудови комбінаторних моделей із застосуванням впорядкованих сукупностей елементів – цілих додатних чисел, лежить в основі поняття "ідеальної кільцевої в'язанки" (ІКВ), що відіграє роль базової моделі для проектування систем з оптимальним розміщенням елементів структури за критерієм досягнення максимальної інформаційної різноманітності системи без збільшення кількості її елементів та зв'язків [2, 3]. Теорія ІКВ та властивості в'язанок лягли в основу нового підходу до проектування технічних пристроїв та систем з поліпшеними якісними характеристиками за такими показниками, як надійність, роздільна здатність, функціональні можливості. Математичні конструкції на впорядкованих елементах, які організовані згідно із вищезгаданим принципом, виявилися зручним інструментом для синтезу та дослідження кругових шкал з нерівномірним розміщенням позначок, що дало змогу підвищити їхню роздільну здатність завдяки зменшенню кроку відліку [4].

Можливість застосування алгебричних методів синтезу кругових шкал випливає з того факту, що структура деяких алгебричних конструкцій і будова кругових шкал з підвищеною роздільною здатністю ґрунтуються на принципі "оптимальних структурних пропорцій" (ОСП), в якому використовуються властивості ІКВ [5]. Основна ідея полягає в оптимальному розміщенні фіксованої кількості позначок на шкалі за критерієм досягнення якнайвищої її роздільної здатності. Один із підходів до вивчення та проектування шкал з підвищеною роздільною здатністю ґрунтується на використанні алгебричних властивостей полів Ґалуа.

Алгебра полів Ґалуа

Для всякого степеня простого числа p і будь-якого $r \geq 1$ існує єдине з точністю до ізоморфізму $GF(p^r)$, тобто поле зі скінченною кількістю елементів або поле Ґалуа, де GF означає *Galois Field.*

З теорії скінченних полів відомо, що поле $GF(p^r)$ можна зобразити як множину всіх класів лишків за модулем довільного полінома $f(x)$ степеня r, незвідного над полем $GF(p)$. Поліном $f(x)$ степеня $r \geq 1$ 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 $f = x^2 - 2$. У цьому доволі легко переконатися, перевіривши, що він не ділиться без залишку на поліноми степеня $r \geq 1$ 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 $s = 1, \quad q = p^r$, то первісним буде такий незвідний над полем $GF(p^r)$ поліном степеня n, корінь якого в полі $GF(p^r)$ має період $p^r - 1$.

У такому разі всі корені полінома $f(x)$ первісні. Кожен відмінний від нуля елемент k поля $GF(q)$ подається у вигляді

$$k = \theta^t. \tag{1}$$

Характеристична функція

$$f_t(x) = f(x; \theta^t) \tag{2}$$

елемента θ^t є поліномом степеня n з коефіцієнтами з $GF(q)$.

У полі $GF(q^s)$ всі його $q^s - 1$ ненульові елементи різні та утворюють циклічну групу за операцією множення. Завдання полягає в тому, щоб дослідити комбінаторні властивості полів Ґалуа, і на основі вивчення їхньої структурної організації розробити алгоритм синтезу шкал з високою роздільною здатністю.

Відомо, що первісний елемент x поля $GF(q^s)$ має максимально можливий період $q^s - 1$ елементів цього поля, а степені x^κ (k=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. Відомо, що 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 $\alpha: x \to x^p$ для будь-якого $x \in GF(q^s)$. Іншими словами, це така взаємна відповідність, за якої корені цього незвідного полінома переводяться в інші корені цього самого полінома. В цьому можна переконатися, побудувавши поля для різних коренів полінома. Так, корені полінома $f(x) \equiv x^2 + x + 2$ є первісними елементами поля $GF(3^2)$. Якщо коренем полінома вибрати первісний елемент x, то отримаємо поле $GF_1(3^2)$, елементами якого є степені x за модулем q=3:

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

Якщо коренем незвідного полінома взяти $x^3 \equiv 2x + 2$, то отримаємо поле $GF_2(3^2)$, елементами якого є степені x за модулем q=3:

$x^0 \equiv 1$

$x^1 \equiv 2x + 2$

$x^2 \equiv x + 2$

$x^3 \equiv x$

$x^4 \equiv 2$

$x^5 \equiv x + 1$

$x^6 \equiv 2x + 1$

$x^7 \equiv 2x$

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

Підполя поля $GF(p^r)$ – це поля $GF(p^m)$, де m ділить r. Для будь-якого r поле $GF(p^r)$ має єдине підполе $GF(p^m)$, що складається з елементів поля $GF(p^r)$, які задовольняють рівняння $z^{p^m} = z$. Первісний елемент x поля $GF(p^r)$ задовольняє рівняння $g(x) = 0$, де $g(x)$ – незвідний над $GF(p^m)$ поліном степеня r/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 сама кількість гіперплощин, причому кожна гіперплощина має $(q^s - 1)/(q - 1)$ різних точок, а утворений на спільних для двох різних гіперплощин підпростір розмірності $r-2$ 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 $G+1=v,\ \ n=k,\ \ R=\lambda$, (де G – кількість градацій робочого діапазону кругової шкали з високою роздільною здатністю, n – кількість поділок, R – кількість усіх можливих способів відтворювання кожної з кутових відстаней на множині натуральних чисел) існує зв'язок [4]:

$$v = G+1 = \frac{q^{s+1}-1}{q-1},\quad k = n = \frac{q^{s}-1}{q-1},\qquad \lambda = R = \frac{q^{s-1}-1}{q-1}, \tag{3}$$

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

Із залежностей (3) легко обчислити степінь полінома, за допомогою якого будується шкала з високою роздільною здатністю. Для симетричної блок-схеми виконується співвідношення:

$$k(k-1) = \lambda(v-1). \tag{4}$$

Відомо, що при $\lambda = 1$ симетрична блок-схема є проективною площиною порядку $k-1$.

Оскільки симетрична блок-схема є циклічною, а точки у будь-якій гіперплощині визначають (v, k, λ) – різницеву множину [1], то досконалу кругову шкалу ($n\rangle 2$) можна розглядати як поле Галуа, в якому є $n-1=p^r$ елементів, що відповідає певній циклічній блок-схемі. Скінченні проективні множини є інструментом для побудови шкал з високою роздільною здатністю, тобто кругових шкал, для яких R=1. Така кругова шкала може являти собою $PG(s,q)$ тільки за умови, що її параметри пов'язані між собою залежностями

$$\begin{aligned} G\ -n &= q^s - 1, \\ n - R &= q^{s-1}. \end{aligned} \tag{5}$$

Залежності (5) дають підстави говорити про можливість проектування шкал з високою роздільною здатністю з параметрами, що відповідають параметрам зінгерових циклічних блок-схем [1].

Алгоритм побудови шкали з високою роздільною здатністю

Алгоритм побудови кругової шкали з кількістю G градацій, кількістю n поділок і "фактором рядності" R=λ передбачає виконання таких дій:

1) вибрати або обчислити деякий незвідний над полем $GF(p^r)$ поліном, враховуючи залежності (5);

2) визначити первісний елемент x цього поля з максимально можливим періодом і обчислити всі його степені x, x^2,…,x^{G+1}, які повинні “пробігати” значення усіх ненульових елементів $GF(p^r)$;

3) за побудованою алгебричною структурою визначити співвідношення кутових відстаней між позначками кругової шкали. Знайдене циклічне співвідношення кутових відстаней є одним із варіантів побудованої досконалої кругової шкали.

Важливо дослідити можливості побудови різних варіантів (інваріантів) кругових шкал з високою роздільною здатністю, щоб можна було порівняти їх між собою та вибрати потрібний.

Проблема побудови шкал за вищеописаним алгоритмом ускладнюється тим, що для різних полів необхідно знаходити інші поліноми, які приводять до побудови однакових варіантів кругової шкали з високою роздільною здатністю. Так, наприклад, побудувавши алгебричні моделі шкал за двома різними первісними поліномами третього степеня ($f_1(x)=x^3-x^2-2$ та $f_2(x)=x^3-2x^2-1$) у полі $GF(p^r)$, r=1, p=3, можна побачити, що "розгортки" обох поліномів відповідають одній і тій самій кільцевій послідовності кутових відстаней між поділками (1,4,6,2), і отже, одному й тому самому варіанту конструкції кругової шкали з високою роздільною здатністю з параметрами n=4, R=1, G=12.

Розглядаючи набори елементів обох алгебричних конструкцій, можна побачити, що порядкові номери i елементів x^i, i =1,2,…,13, в складі яких відсутні доданки одного з трьох (q=3) фіксованих степенів x, визначають співвідношення кутових відстаней між позначками кругової шкали з високою роздільною здатністю з параметрами n=4, R=1, G=12. Наприклад, в обох конструкціях відсутні доданки x^2 в рядках під номерами 1,5,11,13, що відповідає кільцевій послідовності (4,6,2,1), яка визначає співвідношення кутових відстаней між позначками шкали з вказаними параметрами [6].

Проблема полягає в тому, що не завжди вдається підібрати відповідні алгебричні конструкції для побудови шкали з потрібними параметрами. Питання побудови таких шкал ускладнюється ще й тим, що існує нескінченно багато випадків таких конструкцій, які не можна утворити одну з одної методами алгебричних перетворень.

Інша проблема, з якою доводиться стикатися під час побудови кругової шкали з високою роздільною здатністю за допомогою полів Ґалуа, полягає в пошуку незвідного полінома. Один із простих способів знаходження незвідного полінома полягає в побудові супровідної матриці для цього полінома за допомогою обчислення характеристичного визначника матриці, що є степенем іншої матриці. Інші методи передбачають побудову проміжних матриць або використання таблиць найменших первісних коренів або таблиць Бюзі, Марша та інших, які допомагають в пошуку первісних незвідних поліномів [7].

$$\left.\begin{aligned} f_1(x) &\equiv x^3 - x^2 - 2 \\ x &\equiv x \\ x^2 &\equiv x^2 \\ x^3 &\equiv x^2 + 2 \\ x^4 &\equiv x^2 + 2x + 2 \\ x^5 &\equiv 2x + 2 \\ x^6 &\equiv 2x^2 + 2x \\ x^7 &\equiv x^2 + 1 \\ x^8 &\equiv x^2 + x + 2 \\ x^9 &\equiv 2x^2 + 2x + 2 \\ x^{10} &\equiv x^2 + 2x + 1 \\ x^{11} &\equiv x + 2 \\ x^{12} &\equiv x^2 + 2x \\ x^{13} &\equiv 2 \end{aligned}\right\} (\text{modd } x^3\text{-}x^2\text{-}2,3) \qquad \left.\begin{aligned} f_2(x) &\equiv x^3 - 2x^2 - 1 \\ x &\equiv x \\ x^2 &\equiv x^2 \\ x^3 &\equiv 2x^2 + 1 \\ x^4 &\equiv x^2 + x + 2 \\ x^5 &\equiv 2x + 1 \\ x^6 &\equiv 2x^2 + x \\ x^7 &\equiv 2x^2 + 2 \\ x^8 &\equiv x^2 + 2x + 2 \\ x^9 &\equiv x^2 + 2x + 1 \\ x^{10} &\equiv x^2 + x + 1 \\ x^{11} &\equiv x + 1 \\ x^{12} &\equiv x^2 + x \\ x^{13} &\equiv 1 \end{aligned}\right\} (\text{modd } x^3\text{-}2x^2\text{-}1,3)$$

Зазначимо, що всі алгебричні методи синтезу кругових шкал з високою роздільною здатністю, зокрема й з використанням вищезгаданих таблиць, пов'язані з достатньо громіздкими обчисленнями. Тому ці методи доцільно суміщати з комп'ютерними розрахунками.

В основі методу дослідження кругових шкал покладено системний підхід. Йдеться про вивчення такої шкали як системи, що складається з однорідних частин і утворює цілісну структуру. Предметом цієї теорії є встановлення принципів, що справедливі не лише для шкал, але й для інших системних об'єктів незалежно від їхньої фізичної природи та конкретного призначення, наприклад, еталонів мір фізичних та електричних величин або систем кодування та перетворення сигналів. Тому цілком припустимою теоретичною процедурою можна вважати редукцію або зведення різних теорій до єдиної як вираження загальної тенденції до встановлення єдності наукового знання як принципу оптимальних структурних пропорцій (ОСП), на якому ґрунтується загальна теорія шкал з високою роздільною здатністю.

Висновок

Алгебричний метод побудови та дослідження комбінаторних конфігурацій, що ґрунтується на циклічних групах полів Ґалуа та використанні принципу "оптимальних структурних пропорцій", дає змогу проектувати шкали з високою роздільною здатністю для як завгодно великої *a priori* кількості градацій, яке визначається параметрами шкали, пов'язаними з параметрами відповідних класичних комбінаторних конфігурацій. Проблема побудови шкал за вищеописаним алгоритмом ускладнюється певною мірою необхідністю пошуку відповідних поліномів. Однак описаний алгебричний метод розширяє можливості проектування шкал, багатозначних мір та інших вимірювальних засобів з великою кількістю базових мір. Поєднання алгебричних методів та принципу "оптимальних структурних пропорцій" (ОСП) збагачує методологію проектування шкал з високою роздільною здатністю.

1. Холл М. Комбинаторика. – М.: Мир, 1970. 2. Різник В.В. Синтез оптимальних комбінаторних систем. – Львів: Вища школа, 1989. 3. Riznyk V., Bandyrska O. Perspektywy rozwoju metrologii na zasadach teorii "Zlotych pierscieni lichbowych" / Pomiary. Automatyka. Kontrola, vol 53, pr 9 bis / 2007, Krakow, 2007. – S.61–67. 4. Бандирська О.В. Стандартизація безнадлишкових рядів методом оптимальних структурних пропорцій / Автореферат дис.канд.техн.наук. Львів, 2000. 5. Бандирська О.В. Зменшення інформаційної надмірності систем шляхом кодування інформації згідно з принципом оптимальних структурних пропорцій // Метрологія та вимірювальна техніка. Наукові праці V МНТК (Метрологія-2006), т.2, Харків, 2006. – С. 101–105. 6. Велика О.Т. Алгебро-графові моделі синтезу числових кодів з кільцевою структурою / Автореферат дис. канд. техн. наук, 2006. 7. Альберт А.А. Конечные поля // Кибернетический сборник. Вып.3. – М.: Мир, 1966.