УДК 681.3:519.15

О. Велика
Національний університет “Львівська політехніка”,
кафедра електронного машинобудування

СИНТЕЗ КІЛЬЦЕВИХ МОНОЛІТНИХ КОДІВ НА ОСНОВІ МЕТОДУ ГРАФОВИХ ПЕРЕТВОРЕНЬ ЦИКЛІЧНИХ ГРУП ПОЛІВ ГАЛУА

Розроблено новий ефективний метод синтезу монолітних кодів за допомогою використання властивостей циклічних груп у розширених полях Галуа, що розширює можливості вивчення звязків теорії ІКВ з алгебричною теорією скінченних груп у розширених полях Галуа.

The new effective method of synthesis of monolithic codes is developed by the use of properties of cyclic groups in the extended fields of Galois which extends possibilities of study of the connections of theory Ideal Ring Bundles with the algebra theory of cyclic groups in the extensions of Galois fields

Вступ

Комбінаторні моделі та системи широко застосовують у технічній кібернетиці, інформаційно-вимірювальній та обчислювальній техніці, радіотехніці, зв'язку, електротехніці, машинобудуванні, а комбінаторні методи використовують у теорії кодування, математичній логіці, програмуванні, теорії планування експерименту, технічній та статистичній фізиці, економіці, кристалографії, біології. Тому актуальними стали дослідження властивостей існуючих і пошук нових комбінаторних моделей, способів їхньої побудови, класифікація, визначення умов існування, виявлення взаємних зв'язків та інтерпретацій.

Різноманітність алгебричних моделей монолітного коду за існуючої різноманітності їх інтерпретацій через циклічні блок-схеми, різницеві множини, скінченні афінні та проективні площини, матриці Адамара [2] та інші комбінаторні об’єкти вимагають розроблення єдиного підходу до методів синтезу згаданих числових моделей. Один із таких підходів ґрунтується на використанні для побудови коду властивостей полів Галуа та геометрій над ними [1, 3].

Аналіз останніх досліджень

Монолітні коди та методи їхнього синтезу досліджено у багатьох публікаціях. Загальна характеристика таких кодів викладена в монографії [1], де описується кільцевий монолітний код, побудований за правилами розподілу вагових розрядів згідно з послідовністю числового ряду ідеальної кільцевої в'язанки (ІКВ). Для побудови таких кодів доцільно скористатися математичним апаратом теорії скінченних полів та алгебричної теорії чисел. Важливою проблемою, з якою доводиться при цьому стикатись, є побудова первісних незвідних поліномів над полем Галуа.

Вирішити цю проблему можна за допомогою методу супровідних матриць [1, 3], який на основі первісних незвідних поліномів будує ІКВ. Якщо кільцева в’язанка, побудована на основі

вибраного полінома, буде ідеальною, то поліном є первісним незвідним, і за його допомогою можна будувати алгебро-графові моделі монолітного коду.

Постановка задачі

Основним завданням, яке виноситься у статті, є дослідження інваріантності відображення ідеальних кільцевих в'язанок на алгебро-графові моделі кільцевих монолітних кодів та побудова повної сім'ї ІКМК .

Метод розв′язування задачі

Як відомо, первісний елемент *a* поля $GF(q^s)$ має максимально можливий період q^s-1 елементів цього поля, а степені a^k /$k=0,1,...,q^{s-2}$/ пробігають усі ненульові елементи $GF(q^s)$ [2]. Оскільки $a^{q^s-1}=1$, то $a^{q^s}\equiv a$, $a^{q^s+1}\equiv a^2$.... Тому мультиплікативна група поля $GF(q^s)$ є циклічною, причому $q=p^\alpha$, де *p*– просте, а α, s – натуральні числа.

Метод графових перетворень циклічних груп полів Галуа ґрунтується на основі ізоморфних скорочень різницевих множин [1] та встановленої відповідності між ІКВ і різницевими множинами. Різницеву множину можна перетворити в іншу різницеву множину з тими самими параметрами, якщо помножити її елементи на деякий коефіцієнт перетворення [2]. Для того, щоб вибрати коефіцієнти перетворення, потрібно із множини чисел {1,2,3,..., W_n-1), серед яких є множники і коефіцієнти перетворення, виділити останні. Кількість таких коефіцієнтів дає нам змогу визначити кількість перетворень, які можна здійснити над циклічними групами полів Галуа.

Сам алгоритм містить наступні кроки:

1. Задаються параметри ІКМК -n, N і будується кільцевий граф , який відповідає цьому коду;

2. Будується різницева множина з параметрами n, N, S_n , яка однозначно відповідає знайденому ІКМК з такими самими параметрами;

3. Знаходяться коефіцієнти перетворення, які не є множниками цієї різницевої множини;

4. Здійснюючи операцію множення на відповідні коефіцієнти перетворення, знаходимо нові варіанти різницевих множини;

5. На основі знайдених різницевих множин за формулою (3.1) будуються нові ІКМК, які відповідають коду із заданими параметрами, і відповідно будуються нові кільцеві графи та вказуються зв'язки між цими графами .

Контрольний приклад

З допомогою прикладу графічно проілюструємо цей алгоритм.

Нехай нам потрібно побудувати код з параметрами n=6; $N=0$, $W_1=31$

1. Коду із заданими параметрами відповідає послідовність ваг (1,3,2,7,8,10).

2. Будуємо різницеву множину, яка відповідає ІКВ з такими самими параметрами: (0,1,4,6,13,21)

3. Згідно з (3.1) знаходимо коефіцієнти перетворення для цієї різницевої множини. Це будуть числа 1, 2, 3, 4, 8.

4. Здійснюючи операцію множення на відповідні коефіцієнти за модулем 31, знаходимо нові варіанти різницевих множин і упорядковуємо їхні елементи у зростаючому порядку.

а) перемножимо вихідну різницеву множину (0,1,4,6,13,21) на коефіцієнт 2, отримуючи нові різницеві множини, поки не отримаємо знову вихідну множину. Це будуть різницеві множини

(0,1,4,6,13,21)→(0,2,8,11,12,26)→(0,4,16,21,22,24)→
→ (0,1,8,11,13,17)→(0,2,3,16,22,26) →(0,1,4,6,13,21).

б) тепер вихідну множину (0,1,4,6,13,21) так само перемножимо на коефіцієнт 3 і отримаємо такі варіанти

(0,1,4,6,13,21)→(0,1,3,8,12,18)→(0,3,5,9,23,24)→
→ (0,7,9,10,15,27)→ (0,14,19,21,27,30)→ (0,1,4,6,13,21);

в) множимо на коефіцієнт 4 і отримуємо такий набір різницевих множин

(0,1,4,6,13,21)→(0,4,16,21,22,24)→(0,2,3,16,22,26)→
→ (0,2,8,11,12,26)→(0,1,8,11,13,17)→ (0,1,4,6,13,21);

г) перемноживши на коефіцієнт 8, отримуємо такі різницеві множини

(0,1,4,6,13,21)→(0,1,8,11,13,17)→(0,2,8,11,12,26)→
→ (0,2,3,16,22,2)→(0,4,16,21,22,24)→(0,1,4,6,13,21).

5. Далі за формулою (3.1) знаходимо нові варіанти ІКМК, яким відповідатимуть такі вагові розряди

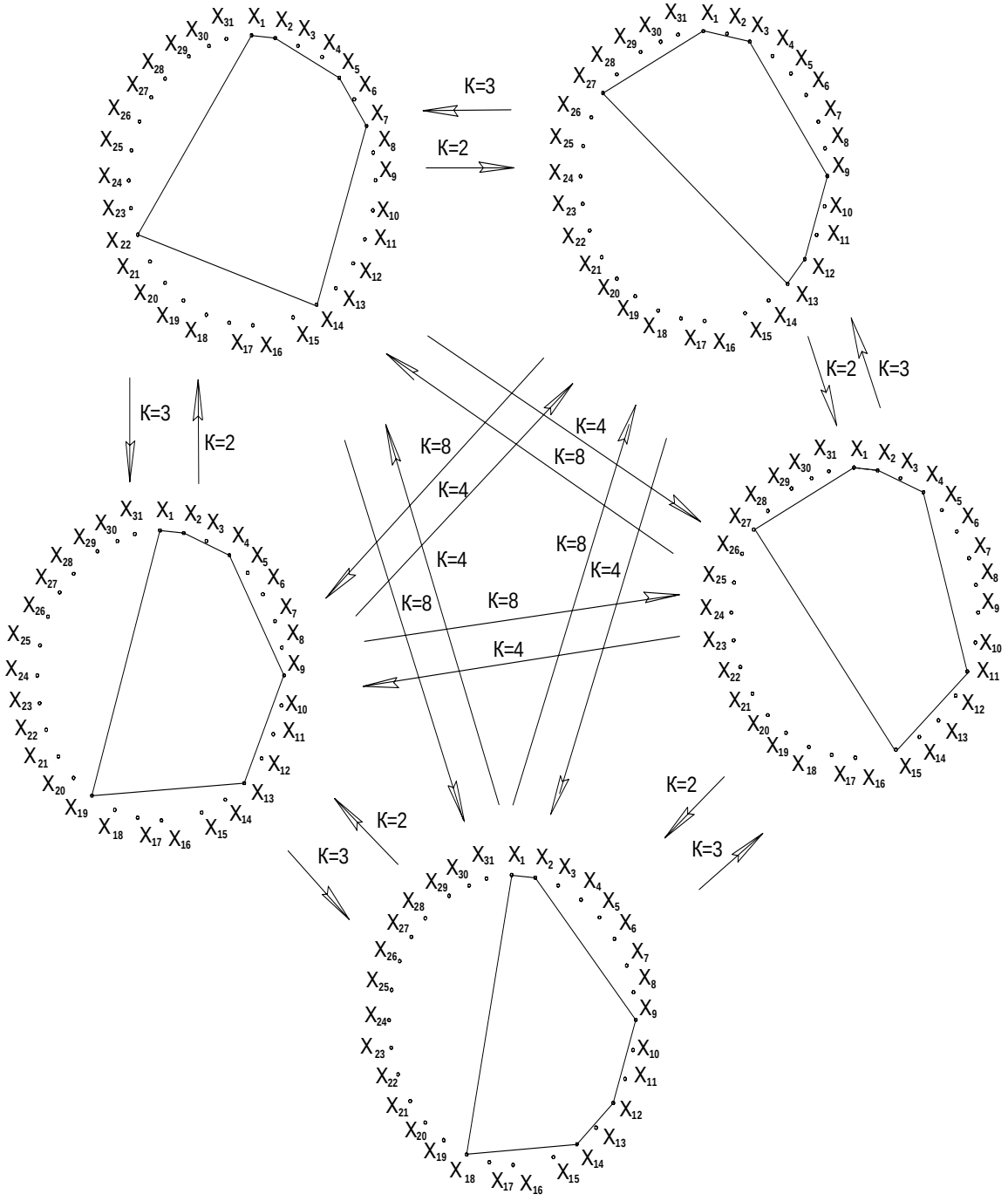
а) (1,3,2,7,8,10)→(1,14,5,2,6,3)→(1,2,7,4,12,5)→
→(1,7,3,2,4,14)→→(1,13,6,4,5,2)→(1,3,2,7,8,10);
б) (1,3,2,7,8,10)→(1,13,6,4,5,2)→(1,7,3,2,4,14)→
→(1,2,7,4,12,5)→→(1,14,5,2,6,3)→ (1,3,2,7,8,10);
в) (1,3,2,7,8,10)→(1,2,7,4,12,5)→(1,13,6,4,5,2)→
→(1,14,5,2,6,3)→→(1,7,3,2,4,14)→(1,3,2,7,8,10);
г) (1,3,2,7,8,10)→(1,7,3,2,4,14)→(1,14,5,2,6,3)→
(1,13,6,4,5,2)→(1,2,7,4,12,5)→(1,3,2,7,8,10).

Будуємо кільцеві графи знайдених ІКМК, а також зв'язки між ними (рисунок), які ілюструють графові перетворення коду із заданими параметрами.

Графові перетворення зручно подати і у вигляді наведеної нижче таблиці, де кожному варіанту відповідає певна графова модель

коеф. перетвор.	1	2	3	4	5	6	7	8
Варіант 1	B1	B 2	B5	B3	B1	B1	B1	B4
Варіант 2	B2	B 3	B1	B4	B2	B2	B2	B5
Варіант 3	B3	B4	B2	B5	B3	B3	B3	B1
Варіант 4	B4	B5	B3	B1	B4	B4	B4	B2
Варіант 5	B5	B1	B4	B2	B5	B5	B5	B3

Метод графових перетворень циклічних груп полів Галуа є дуже ефективний, оскільки для побудови повної сім'ї ІКМК достатньо знайти хоча б один із варіантів ІКМК із заданими параметрами, а далі, здійснюючи операцію множення на коефіцієнти перетворення, можна відшукати всі можливі варіанти ІКМК. Результати досліджень вказують, що при збільшенні порядку n збільшується кількість коефіцієнтів, а отже, зростає кількість перетворень.



Графові перетворення ІКМК з параметрами n *=6;* $N = 0$

Висновок

Дослідження відображення кільцевих монолітних кодів на циклічні алгебро-графові структури розширює можливості вивчення зв′язків теорії ідеальних кільцевих в′язанок (ІКВ) з алгебричною теорією скінченних груп у розширених полях Галуа та дає змогу розробляти на основі цих відображень нові ефективні методи синтезу монолітних кодів на ідеальних кільцевих в′язанках.

Розроблений новий метод побудови ІКМК з використанням графічних моделей циклічних груп полів Галуа дає змогу побудувати всі без винятку варіанти ІКМК із заданими параметрами.

1. Різник В.В. Синтез оптимальних комбінаторних систем. –Львів: Вища школа, 1989. – 168 с. 2. Свердлик М.Б. Оптимальные дискретные сигналы. – М.: Сов. радио, 1975. – 200 с.3. Велика О. Алгебро-графові моделі синтезу числових кодів з кільцевою структурою: Дис. ... канд. техн. наук: 01.05-02. – Львів, 2006. – 179 с.