

АЛГОРИТМ ПОБУДОВИ БАГАТОМІСНИХ ОРТОГОНАЛЬНИХ КВАЗІГРУП НАД ПОЛЕМ ЛИШКІВ

Вінницький національний технічний університет

Анотація

У даній праці наведено алгоритм побудови n -вибірки ортогональних n -арних лінійних квазігрупових операцій, які визначені над $GF_{(p)}$, де p - просте число. Ортогональні квазігрупи мають важливе прикладне значення: в теорії планування проведення експериментів, у криптографії, при побудові кодів, які виправляють помилки тощо.

Ключові слова: Оборотна матриця, визначник, ортогональність, лінійна квазігрупа.

Abstract

This paper presents an algorithm for constructing a n -sample of orthogonal n -ary linear quasigroup operations defined over $GF_{(p)}$, where p is a prime number. Orthogonal quasigroups have important applied significance: in the theory of experiment planning, in cryptography, in the construction of error-correcting codes, etc.

Keywords: Invertible matrix, determinant, orthogonality, linear quasigroup.

Вступ

Ортогональність операцій має важливе прикладне значення. Цьому питанню присвячено багато праць. Зокрема Г. Манном у праці [3] описано побудову бінарних ортогональних операцій. Л. Пейджем [4] і М. Холлом [5] було знайдено необхідні і достатні умови існування ортогональної пари для груп. Результати дослідження ортогональних багатомісних квазігруп викладено у праці [1] С. Муратходжаєва. Білявська Г. та Муллен Г. у праці [6], а також Сохацький Ф. та Фриз І. у праці [8] досліджували властивості ортогональних багатомісних операцій та дано алгоритми їх побудови. Алгоритми побудови багатомісних операцій досліджували Смайл Марковські та Александра Мілева у праці [11]. Алгоритми побудови пари латинських ортогональних квадратів, як еквівалента квазігруп, описано Д. Кідвелом у праці [7]. В даній праці викладені алгоритми побудови систем ортогональних квазігрупових операцій при $n > 2$.

1 Додаткові відомості

Нагадаємо, що операція f , яка визначена на множині Q , називається i -оборотною, якщо для довільних елементів $a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_n$ із Q існує єдиний елемент $x \in Q$ такий, що $f(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n) = b$.

Операція f називається *оборотною* або *квазігруповою*, якщо вона i -оборотна для всіх $i \in \overline{1, n}$. Тоді пару $(Q; f)$ називають *квазігрупою*, точніше *n -арною квазігрупою*.

Групові ізотопи. [2] n -арний групоїд $(Q; f)$ називається *груповим ізотопом*, якщо існує група $(G; +)$ та бієкції $\alpha_1, \dots, \alpha_n, \alpha_{n+1}$ із Q на G такі, що виконується рівність $f(x_1, \dots, x_n) = \alpha_{n+1}^{-1}(\alpha_1 x_1 + \dots + \alpha_n x_n)$, для всіх $x_1, \dots, x_n \in Q$.

Отже, n -арний групоїд $(Q; f)$ є *квазігрупою*, якщо операція f оборотна.

Означення 1. [2] Нехай $(Q; f)$ n -арний груповий ізотоп і нехай $(Q; +, 0)$ - група, $\alpha_1, \dots, \alpha_n$ -

При умові, що $(\det A - (a_{i1}A_{i1} + \dots + a_{i(i-1)}A_{i(i-1)})) \in \mathbb{Z}_m^*$. Де A_{ij} - відповідні алгебричні доповнення, та

$A_{ii} \in \mathbb{Z}_m^*$, для всіх $i = 2, \dots, n$.

3. Алгоритм побудови n -вибірки ортогональних лінійних n -арних квазігруп

Як зазначалося у Розділі 2: задача про побудову n -вибірки ортогональних n -арних квазігруп, які визначені в $GF_{(p)}$, зводиться до побудови оборотних матриць розмірності $n \times n$, які складаються із ненульових елементів поля.

Розглянемо $GF_{(p)}$, де p - просте число, $a_{ij} \in GF_{(p)}^*$. Тоді оборотна матриця розмірності $n \times n$, яка складається із ненульових елементів поля, будується за такими кроками:

Алгоритм 1.

Крок 1. Елементи a_{ij} - обираються довільним чином із $GF_{(p)}^*$, крім a_{ii} , де $i \in \{2, \dots, n\}$;

Крок 2. Кожен елемент a_{ii} , де $i \in \{2, \dots, n\}$ - обирається довільним чином із $GF_{(p)}^*$, при умові, що $a_{ii} \neq -(a_{i1}A_{i1} + \dots + a_{i(i-1)}A_{i(i-1)})A_{ii}^{-1}$.

Савчук Віктор Дмитрович, асистент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця. svit0118@gmail.com

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Муратхуджаев С. Допустимость n -квазигрупп. Связь допустимости и ортогональности // Мат. Исслед – 1985. – № 83. – С. 77-86.
2. Сохацкий Ф. Н., Кирнасовский О. Е. Кононические разложения многоместных изотопов групп. Известия Гомельского государственного университета им. Ф. Скорины. Вопросы алгебры. – 2001. – № 3(6) – 17. – С. 88-97.
3. Mann H.B. The construction of orthogonal Latin squares. Ann. Math. Statist. – 1942. – 13, P – 418-423.
4. Paige L.J. A note on finite abelian groups. Bull. Amer. Math. Soc. – 1947. – 53.
5. Hall M. A combinatorial problem on Abelian groups. Proc. 34 Amer. Math. Soc. – 1952. – 3.
6. Belyavskaya G., Mullen G. L. Orthogonal hypercubes and n -ary operations. Qasigroup Related Systems 13(2005), no. 1, 73-86.
7. Keedwell D., Denes J. Latin Squares and their Applications // Second Edition – 2015. – P. 440.
8. Fryz I.V., Sokhatsky F.M. Block composition algorithm for constructing orthogonal n -ary operations // Discrete Math – 2017. – № 340. – P. 1957--1966.
<http://dx.doi.org/10.1016/j.disc.2016.11.012>
9. Fryz I.V. Orthogonality and retract orthogonality of operations // Bul. Acad. Stiinte Repub. Mold. Mat – 2018. – № 1(86). – P. 24-33.
10. Fryz I.V. Algorithm for the complement of orthogonal operations // Comment. Math. Univ. Carolin – 2018. – № 59,2. – P. 135-151. <http://dx.doi.org/10.14712/1213-7243.2015.241>
11. Markovski S., Mileva A. On construction of orthogonal d -ary operations // De L'institute masemateque. Nouvelle serie – 2017–№ 101(115). – P. 109-119.