**Конференція молодих учених «Підстригачівські читання – 2020»,
26–28 травня 2020 р., Львів**

УДК 512.548.7

АЛГОРИТМ ПОБУДОВИ *N*–АРНИХ ОРТОГОНАЛЬНИХ ЛІНІЙНИХ КВАЗІГРУП НАД $GF_{(p)}$

Віктор Савчук

Інститут прикладних проблем механіки і математики ім. Я. С. Підстригача
НАН України, savchukvd@ukr.net

Нехай всі операції визначені на одній і тій же множині, позначемо її Q.

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

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

Групові ізотопи. [1] n-арний групоїд $(Q;f)$ називають *груповим ізотопом*, якщо існує група $(G;+)$ та бієкції $\alpha_1,...,\alpha_n,\alpha_{n+1}$ із Q на G такі, що виконується рівність $f(x_1,...,x_n)=\alpha_{n+1}^{-1}(\alpha_1 x_1+...+\alpha_n x_n)$, для всіх $x_1,...,x_n \in Q$. Отже n-арний групоїд $(Q;f)$ є квазігрупою, якщо операція f оборотна. Групоїд $(Q;f)$ називається: *n-аним бінарної* групи, якщо $f(x_1,...,x_n):=x_1+...+x_n$; *груповим ізотопом*, якщо він ізотопний n-арній похідній деякої бінарної групи; *лінійним* над групою, якщо він є груповим ізотопом цієї групи, причому компоненти ізотопізму є її лінійними перетвореннями; *центральною квазігрупою* або *T-квазігрупою*, якщо він лінійний над деякою комутативною групою.

Ортогональність n-арних лінійних квазігруп. n-арні лінійні операції $f_1,...,f_n$, які визначені на множині Q називають ортогональними, якщо система

$$\begin{cases} f_1(x_1,...,x_n)=a_{11}x_1+...+a_{1n}x_n=b_1, \\ f_2(x_1,...,x_n)=a_{21}x_1+...+a_{2n}x_n=b_2, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ f_n(x_1,...,x_n)=a_{n1}x_1+...+a_{nn}x_n=b_n, \end{cases} \qquad (1)$$

має єдиний розв'язок, для всіх $b_1, b_2, ..., b_n \in Q$.

З іншого боку система (1) має єдиний розв'язок, якщо матриця

$$\begin{pmatrix} a_{11} & ... & a_{1n} \\ ... & ... & ... \\ a_{n1} & ... & a_{nn} \end{pmatrix} \tag{2}$$

оборотна в Q .

Нехай $Q = GF_{(p)}$, а $GF^*_{(p)}$ - множина ненульових елементів $GF_{(p)}$. Тоді задача про побудову n -вибірки n -арних лінійних ортогональних квазігруп зводиться до побудови оборотної матриці $n \times n$ із ненульовими елементами $GF_{(p)}$. Скориставшись наслідком до теореми Лапласа про розклад визначника встановлено таку теорему:

Теорема 1. *Нехай (2) – $n \times n$ матриця, де $a_{ij} \in GF^*_{(p)}$. Тоді (2) є оборотною в $GF_{(p)}$ тоді і тільки тоді, коли для всіх $a_{ij} \in GF^*_{(p)}$ та для $i \in 2, ..., n$, кожне*

$$a_{ii} \neq (a_{i1}M_{i1} + ... + a_{i(i-1)}M_{i(i-1)})M_{ii}^{-1} .$$

Алгоритм 1.

Крок 1. Елементи $a_{ij} \in GF^*_{(p)}$ – обираються довільним чином, крім елементів a_{ii} , де $i \in 2, ..., n$;

Крок 2. Елементи a_{ii} , де $i \in 2, ..., n$ – обираються довільним чином із $GF^*_{(p)}$, при умові, що $a_{ii} \neq (a_{i1}M_{i1} + ... + a_{i(i-1)}M_{i(i-1)})M_{ii}^{-1}$.

1. *Сохацкий Ф. Н., Кирнасовский О. Е.* Канонические разложения многоместных изотопов групп. Известия Гомельского государственного университета им. Ф. Скорины. Вопросы алгебры. – 2001. – №3(6). – С. 88 – 97.
2. *Keedwell D., Denes J.* Latin Squares and their Applications// Second Edition – 2015. – P. 440.

AN ALGORITHM OF CONSTRUCTION OF N – ARY ORTHOGONAL LINEAR QUASIGROUPS ON $GF_{(p)}$

D. Kidwell in [2] described algorithms for constructing a pair of orthogonal Latin squares (orthogonal binary quasigroups). In this paper, we propose an algorithm for constructing an n −tuple n -ary of orthogonal quasigroups, defined on $GF_{(p)}$.