КРИПТОСТОЙКОСТЬ ДИАССОЦИАТИВНЫХ КВАЗИГРУПП 4-ГО ПОРЯДКА

Комилов О.О.
Таджикский национальный университет
https://doi.org/ 10.5281/zenodo.17331042

В работе исследуются конгруэнция и простота диассоциативных квазигрупп 4-го порядка степени 3. Конгруэнции в современной криптографии обеспечивают математическую основу для защиты информации и имеет важное значение для структуры любой группы и квазигруппы. Автором приведены примеры конгруэнции для квазигрупп 4-го порядка. Доказана, что для квазигруппы с тождеством диассоциативности не существует нетривиальной конгруэнции, что имеет важное значение для структуры этой квазигруппы.

Конгруэнции являются важным понятием в теории алгебр. Они позволяют изучать структуру алгебр через отношение эквивалентности, которое согласовано с операциями алгебры. В теории групп и квазигрупп примеры конгруэнции связаны с нормальными подгруппами и факторгрупп.

Изучением конгруэнциям занимались многие классики математики, как Р.Дедекинд [1] и Э.Нётер [2]. Их работы заложили основы для понимания конгруэнции, хотя они не использовали этот термин в современном смысле. Ими изучались понятия идеалы, гомоморфизмы и фактор-кольца и они оказали огромное влияние на универсальную алгебру, где конгруэнции стали центральными понятием.

Основной целью данной работы является исследование конгруэнций, простоты и криптостойкости диассоциативных квазигрупп малого порядка. В связи с этим формулируются задачи о анализе структуры конгруэнции в диассоциативных квазигрупп малого порядка, исследование простоты этих классов квазигрупп и применении данных квазигрупп в разработке симметричных шифрах.

Одной из наиболее подходящих алгебраических структур для создания криптосистем являются конечные простые квазигруппы, так как их структура не может быть разложена на более простые компоненты, что даст устойчивость к алгебраических атакам. Если в квазигруппе существует нормальная конгруэнция, можно построить факторквазигруппу, что значит исходная квазигруппа не является простой. И если нет нетривиальных нормальных конгруэнций, то квазигруппа простая. Так как, если аргументы операции окажутся элементами подквазигруппы, тогда исходный результат не выйдет за пределы подквазигруппы и сокращается пространство перебора. Этим упрощается процесс взлома. И такие квазигруппы связаны с отсутствием нетривиальных конгруэнций. Идентификация и анализ таких квазигрупп всё еще остается проблемой исследования.

Определение 1. [3] Эквивалентность θ является конгруэнцией группоида $(Q,\cdot)$, если следующие импликации верны для всех $a, b, c \in Q$:

$$a\ \theta\ b\ \Rightarrow (c\ \cdot a)\ \theta\ (c\ \cdot b),\ a\ \theta\ b\ \Rightarrow (a\ \cdot c)\ \theta\ (b\ \cdot c). \qquad (1)$$

Конгруэнция θ нормальна, если для всех $x, y, z \in Q$ верны импликации:

$$(c\ \cdot a)\ \theta\ (c\ \cdot b) \Rightarrow a\ \theta\ b, (a\ \cdot c)\ \theta\ (b\ \cdot c) \Rightarrow a\ \theta\ b. \qquad (2)$$

Когда тип конгруэнции касается двух пар чисел, также можно проверить конгруэнции по следующим условием:

$a, b, c, d \in Q$ если $a\theta b$ и $c\theta d \Rightarrow ac\ \theta\ bd.$ (3)

Пример 1. Пуст $(Q,\cdot)$ группоид представленной в следующей таблице Кэли:

Таблица 1. Группоид $(Q,\cdot)$ 4-го порядка

Table 1. Groupoid $(Q,\cdot)$ of the 4th order

·	1	2	3	4
1	1	3	4	2
2	3	1	2	4
3	4	2	1	3
4	2	4	3	1

Очевидно, что $(Q,\cdot)$ квазигруппа 4-го порядка, диассоциативная степени 3 и коммутативна. То есть в $(Q,\cdot)$ выполняются следующие тождества:

1. $\forall x, y \in Q, \quad ((\,(xy)y)y = x,\ y(y(yx));$
2. $\forall x, y \in Q, \quad xy = yx.$

Как и в предыдущем примере, для нахождения конгруэнции для этой квазигруппе находим все возможные отношение эквивалентности, которые считаются разбиением Q на классы эквивалентности:

Тривиальные разбиение **(**универсальная и тождественная конгруэнция):

{1,2,3,4} - все элементы объединены в один класс эквивалентности;

{1}{2}{3}{4} —каждый элемент образует свой класс эквивалентности:{1}{2}{3}{4};

Нетривиальные разбиение:

Разбиение на два класса вида $\{a, b\}, \{c, d\}$ для всех возможных пар ;

Разбиение на два класса вида $\{a, b, c\}, \{d\}$, где $a, b, c, d \in Q$;

Разбиение на три класса вида $\{a, b\}, \{c\}, \{d\}$, где $a, b, c, d \in Q$.

Проверка согласованности с операцией

Теперь для каждого разбиения можно проверит конгруэнцию, нужно убедится, что для любых $a\theta b$ и $c\theta d$ выполняются условия (1) и (3).

Проверка показала, что в нем все отношение нетривиальных разбиений не являются конгруэнциями.

Видно что, коммутативная диассоциативная квазигруппа 4-го порядка степени 3 $(Q,\cdot)$ не имеет нетривиальных конгруэнций в виде разбиение по классам.

В работе [4] авторам были найдены все диассоциативные квазигруппы 4-го порядка степени 3 в виде латинского квадрата (рисунок 1):

Рисунок 1. Все диассоциативные квазигруппы в виде латинского квадрата

Figure 1. All diassociative quasigroups in the form of a Latin square

1 3 4 2	2 3 1 4	3 1 2 4	4 1 3 2
3 1 2 4	3 2 4 1	1 3 4 2	1 4 2 3
4 2 1 3	1 4 2 3	2 4 3 1	3 2 4 1
2 4 3 1	4 1 3 2	4 2 1 3	2 3 1 4
1	**5**	**9**	**13**
1 3 4 2	2 3 1 4	3 1 2 4	4 1 3 2
4 2 1 3	4 1 3 2	2 4 3 1	2 3 1 4
2 4 3 1	3 2 4 1	4 2 1 3	1 4 2 3
3 1 2 4	1 4 2 3	1 3 4 2	3 2 4 1
2	**6**	**10**	**14**
1 4 2 3	2 4 3 1	3 2 4 1	4 2 1 3
3 2 4 1	3 1 2 4	1 4 2 3	1 3 4 2
4 1 3 2	1 3 4 2	2 3 1 4	3 1 2 4
2 3 1 4	4 2 1 3	4 1 3 2	2 4 3 1
3	**7**	**11**	**15**
1 4 2 3	2 4 3 1	3 2 4 1	4 2 1 3
4 1 3 2	4 2 1 3	2 3 1 4	2 4 3 1
2 3 1 4	3 1 2 4	4 1 3 2	1 3 4 2
3 2 4 1	1 3 4 2	1 4 2 3	3 1 2 4
4	**8**	**12**	**16**

Следствие. В диассоциативной квазигруппе 4-го порядка степени 3 поскольку нет нетривиальных разбиений, сохраняющих операцию квазигруппы, нет и нетривиальных конгруэнций. Следовательно, квазигруппа простая.

Refrences:

1. Дедекинд Р. Доклады по теории чисел / Р. Дедекинд // Брауншвейг.:изд. Фридриха Вевега. 1863. – С. 438.
2. Нётер Э. Идеальная теория в кольцевых областях / Э.Нётер // Математические анализ. Т. 83(1). 1921. – С. 24-66
3. Белоусов В.Д. Основы теории квазигрупп и луп [Текст] / В.Д. Белоусов // М.: Наука. 1967. – С. 223
4. Комилов О.О. Диассоциативные квазигруппы малого порядка /О.О. Комилов // Доклады НАН Таджикистана. 2020. Том 63. № 11-12. – С. 665 – 671.