**Московский государственный университет**
**имени М.В.Ломоносова**

Механико-математический факультет

Кафедра Математической теории интеллектуальных систем

# КУРСОВАЯ РАБОТА

Анализ свойств квазигрупп, порожденных некоторыми классами перестановок с полным дифференциалом
Investigation of properties of quasigroups generated by some classes of full difference permutations

Выполнил студент 5 курса:
Р.А.Жигляев
Научный руководитель:
к.ф.-м.н., с.н.с. А.В.Галатенко

Москва, 2022

**Аннотация**

Работа посвящена генерации случайных квазигрупп на основе подстановок с полным дифференциалом. Рассматриваются два варианта таких подстановок — регистры сдвига и обобщенные сети Фейстеля. Приводится описание программной реализации генератора и результаты экспериментов по проверке свойств полученных квазигрупп.

The work is devoted to the generation of random quasigroups based on substitutions with a total differential. Two variants of such substitutions are considered - shift registers and generalized Feistel networks. A description of the software implementation of the generator and the results of experiments to test the properties of the obtained quasigroups are given.

# 1. Введение

Неассоциативные и некоммутативные алгебраические объекты представляют особый интерес в криптографии. Одним из примеров таких объектов могут выступать конечные квазигруппы. На основе квазигрупп можно построить большое количество различных шифров и хэш-функций [1].

Стойкость криптоалгоритмов можно увеличить за счет нескольких идей. Первая идея заключается в том, чтобы выбирать достаточно большие по размеру квазигруппы. Однако, такой подход может вызвать проблемы в связи с ограниченностью памяти компьютера. Вариантом решения этих проблем может быть задание квазигрупп с помощью функций. Например, как показано в [2], можно задавать квазигруппу с помощью подстановок с полным дифференциалом. Еще одним плюсом функционального задания квазигрупп может быть более быстрая генерация квазигрупп большого размера.

Вторая идея заключается в выборе тех квазигрупп, которые обладают набором интересных свойств. К таким свойством можно отнести неаффиность и простоту, или что тоже самое - полиномиальную полноту [3]. Как известно, почти все квазигруппы являются полиномиально полными [4], поэтому выбор случайной квазигруппы с большой долей вероятности может оказаться успешным.

Наконец, еще одним важным фактором является получение таких квазигрупп, которые не имеют подквазигрупп, так как в противном случае произведение элементов подквазигруппы не будет выходить за пределы этой подквазигруппы.

В задачи данной работы входит разработка программы, которая будет генерировать квазигруппы на основе подстановок с полным дифференциалом. А именно - будут рассмотрены регистры сдвига и обобщенные сети Фейстеля. Разработка программы ведется на языке C++. Сгенерированные объекты проверяются на полиномиальную полноту, а также выясняется наличие у них подквазигрупп. Все эксперименты проводились на компьютере Intel(R) Core(TM) i5-11400H @ 2.70GHz, 8ГБ ОЗУ.

В результате будет представлено описание программы и оценка сложности алгоритма.

Работа устроена следующим образом: в разделе 2 даны основные определения; в разделе 3 даны описания алгоритмов генерации квазигрупп на основе регистров сдвига и обобщенных сетей Фейстеля; раздел 4 посвящен экспериментам с программой; в разделе 5 подводятся итоги работы.

# 2. Основные определения

**Определение 1.** Конечное множество $Q$, на котором задана бинарная операция умножения $f_Q$: $Q \times Q \to Q$, такая, что для любых элементов $a, b \in Q$ уравнения $ax = b$ и $ya = b$ однозначно разрешимы в $Q$, называется *конечной квазигруппой*. Операцию $f_Q$ будем называть квазигрупповой.

Операцию $f_Q$ также можно задать с помощью таблицы умножения, которая будет представлять из себя латинский квадрат.

**Определение 2.** Квазигруппа $(Q, f_Q)$ называется аффинной, если на множестве $Q$ можно ввести структуру абелевой группы $(Q, +)$, такую, что существуют автоморфизмы $\alpha$, $\beta$ группы $(Q, +)$ и элемент $c \in Q$, для которых выполнено тождество

$$f_Q(x, y) = \alpha(x) + \beta(y) + c.$$

**Определение 3.** Квазигруппа $(Q, f_Q)$ называется простой, если операция $f_Q$ не сохраняет никакое нетривиальное разбиение Q.

Как уже было сказано ранее - неаффинные и простые квазигруппы будем называть полиномиально полными.

**Определение 4.** Пусть $Q' \subset Q$, $1 \leq |Q'| < |Q|$. Если $f_Q(Q') = Q'$, то будем говорить, что квазигруппа $(Q, f_Q)$ содержит собственную подквазигруппу $(Q', f_{Q'})$, где $f_{Q'}$ - ограничение операции $f_Q$ на $Q' \times Q'$. Если $|Q'| \geq 2$, то такую подквазигруппу будем называть нетривиальной.

**Определение 5.** Пусть задана конечная абелева группа $(G; +)$, а $\sigma$ некоторая подстановка на множестве $G$. Подстановку $\sigma$ будем называть полной над группой $(G; +)$, если функция $\sigma(x) - x$ является биекцией.

Полные подстановки также будем называть подстановками с полным дифференциалом. Связь между квазигрупповыми операциями и полными подстановками задается следующим образом:

$$f_Q(x, y) = \sigma(x + y) - y.$$

Отметим также конструкции, которые будем использовать в дальнейшем. Следующее соотношение будем называть регистром сдвига с обратной связью:

$$\begin{cases} f_1 = x_2 \\ f_2 = x_3 \\ ... \\ f_{n-1} = x_n \\ f_n = x_1 + g(x_2, ..., x_n) \end{cases}$$

Выбрав некоторые положительные целые числа $k, n$ и представив элементы $x, y, z \in Q$, такие, что $z = f_Q(x, y)$ в виде $k$-ичных векторов $(x_1, ..., x_n)$, $(y_1, ..., y_n)$, $(z_1, ..., z_n)$ соответственно, можно задать квазигруппу с помощью регистров сдвига следующим образом:

$$\begin{cases} z_1 = x_2 + y_2 - y_1 \\ z_2 = x_3 + y_3 - y_2 \\ ... \\ z_{n-1} = x_n + y_n - y_{n-1} \\ z_n = x_1 + y_1 + g(x_2 + y_2, ..., x_n + x_n) - y_n \end{cases}$$

Для случая, когда $n = 2$ рассмотрем так же конструкцию, называемую обобщенной сетью Фейстеля:

$$\begin{cases} f_1 = s(x_2) \\ f_2 = x_1 + p(x_2) \end{cases}$$

Здесь $s$ и $p$ - две перестановки из $k$ элементов. Квазигруппу из такой конструкции можно получить по формулам:

$$\begin{cases} f_1 = s(x_2 + y_2) - y_1 \\ f_2 = x_1 + y_1 + p(x_2 + y_2) - y_2 \end{cases}$$

Обе конструкции, однако, не всегда позволяют получить квазигруппы. Необходимые для этого условия на функции $g, s, p$ были даны в [5]. В более узкой постановке идея расширения сетей Фейстеля также представлена в [6].

Порядок генерируемых квазигрупп будем обозначать как $N$. Все сложения и вычитания происходят по модулю $k$.

# 3. Описание алгоритмов генерации

Рассмотрим для начала обобщение сетей Фейстеля. Для этого необходимо лишь сгенерировать две случайные перестановки $s$ и $s'$. Сделать это можно, например, используя алгоритм Фишера-Йетса. После генерации обеих перестановок можно вычислить функцию $p(x) = s'(x) - s(x) + x$. Общая сложность всех преобразований составляет $O(3k)$ или $O(3\sqrt{N})$. При этом, обе перестановки $s$ и $p$ однозначно задают квазигруппу. Следовательно, сложность алгоритма по памяти составляет $O(2k)$ или $O(2\sqrt{N})$.

Если потребуется вычисление всего латинского квадрата, то для вычисления каждого конкретного значения $f_Q(x, y)$ потребуется преобразовать $x$ и $y$ в $k$-ичные векторы $(x_1, x_2)$ и $(y_1, y_2)$ соответственно. После этого необходимо вычислить вектор $(f_1, f_2)$ и преобразовать этот $k$-ичный вектор в $f_Q(x, y)$. Все эти операции выполняются с константной сложностью, а значит, сложность преобразования обобщенных сетей Фейстеля в латинский квадрат составляет $O(N^2)$.

Рассмотрим теперь алгоритм генерации регистров сдвига. Весь алгоритм заключается в генерации функции $g$ из которой однозначно можно получить некоторую квазигруппу. Будем перебирать все наборы вида $(0, x_3, ..., x_n)$. Для каждого такого набора сгенерируем случайную перестановку $(p_0, ..., p_{k-1})$. После этого зададим значение функции g на наборе $(i, x_3+i, ..., x_n+i)$ равным $p_i$. Таким образом получится функция $g$, такая, что любой нетривиальный сдвиг будет менять её значение. При такой функции $g$ регистр сдвига с обратной связью будет являться подстановкой с полным дифференциалом и задавать квазигруппу.

Программно алгоритм выглядит так:
1) Перебираем числа от 0 до $k^{n-2} - 1$.
2) Каждое из них преобразуем в $k$-ичный вектор $(x_2, ..., x_n)$.
3) После этого формируем новый $k$-ичный вектор $(0, x_2, ..., x_n)$.
4) Генерируем перестановку алгоритмом Фишера-Йетса.
5) Перебирая числа от 0 до $k - 1$ формируем набор, на котором хотим задать значение функции g.
6) Преобразуем этот набор в десятичное представление и задаем на нём значение функции g.
Общая временная сложность такого алгоритма составит:

$$O(k^{n-2}(2n - 4 + k(2n - 1))).$$

Сложность алгоритма по памяти составляет $O(k^{n-1})$, так как потребуется хранить $k^{n-1}$ значений функции $g$.

Если потребуется преобразовать регистры сдвига в латинский квадрат, то для этого необходимо для каждого значения функции $f_Q(x, y)$ преобразовать оба аргумента в $k$-ичные векторы длины $n$, вычислить $k$-ичный вектор $(f_1, ..., f_n)$, используя значения функции $g$ и преобразовать этот вектор в $f_Q(x, y)$. Общая временная сложность такого преобразования составит $O(5nk^{2n})$.

# 4. Эксперименты

## Скорость генерации

Эксперимент направлен на оценку времени, за которое можно получить достаточно большие квазигруппы. Для этого генерировались по 10 квазигрупп и замерялось среднее время генерации для различных значений $k$ и $n$.

В таблице ниже приведены результаты эксперимента для квазигрупп на основе регистров сдвига. Время указано с учетом вычисления всех элементов латинского квадрата.

| $k$ | $n$ | Порядок квазигруппы | Время генерации в секундах |
|---|---|---|---|
| 2 | 10 | 1024 | 0.69392 |
| 2 | 11 | 2048 | 3.05952 |
| 2 | 12 | 4096 | 13.3623 |
| 2 | 13 | 8192 | 58.0302 |
| 2 | 14 | 16384 | 255.775 |
| 2 | 15 | 32768 | 1084.45 |
| 4 | 5 | 1024 | 0.304413 |
| 4 | 6 | 4096 | 6.06056 |
| 4 | 7 | 16384 | 116.242 |
| 8 | 4 | 4096 | 3.46345 |

Можно заметить, что при фиксированном порядке квазигруппы время генерации уменьшается с ростом $k$.

Аналогичная таблица для квазигрупп, полученных из обобщенных сетей Фейстеля:

| $k$ | Порядок квазигруппы | Время генерации в секундах |
|---|---|---|
| 16 | 256 | 0.003375 |
| 24 | 576 | 0.015923 |
| 32 | 1024 | 0.050627 |
| 40 | 1600 | 0.121838 |
| 48 | 2304 | 0.263974 |
| 56 | 3136 | 0.48076 |
| 64 | 4096 | 0.804098 |
| 72 | 5184 | 1.30104 |
| 80 | 6400 | 1.93981 |
| 88 | 7744 | 2.73405 |

Можно заметить, что обобщенные сети Фейстеля позволяют генерировать квазигруппы заметно быстрее, чем регистры сдвига. Однако, оба алгоритма показывают себя весьма хорошо и позволяют получать квазигруппы больших размеров достаточно быстро.

## Проверка полиномиальной полноты

Проверка аффинности и простоты проводилась с использованием алгоритмов, описанных в [7]. Поскольку число квазигрупп для обоих методов известно и составляет $(k!)^2$ для сетей Фейстеля и $(k!)^{k^{n-2}}$ для регистров сдвига, можно породить их все для небольших порядков. Для того, чтобы получить все квазигруппы нужного порядка, можно сгенерировать достаточно большое количество объектов и хранить их в unordered set. В силу особенностей unordered set, каждый новый сгенерированный объект не будет добавлен в эту структуру данных, если он в ней уже присутствует. Таким образом, можно генерировать квазигруппы до тех пор, пока число объектов в unordered set не станет равно числу квазигрупп заданного порядка. Далее, перебирая все сгенерированные объекты, можно проверить их на аффинность и простоту.

Результаты эксперимента для регистров сдвига:

| $k$ | $n$ | Всего квазигрупп | Простых | Аффинных |
|---|---|---|---|---|
| 2 | 2 | 2 | 2 | 2 |
| 2 | 3 | 4 | 4 | 0 |
| 2 | 4 | 16 | 14 | 0 |
| 2 | 5 | 256 | 252 | 0 |
| 3 | 2 | 6 | 6 | 0 |
| 3 | 3 | 216 | 210 | 0 |
| 4 | 2 | 24 | 16 | 0 |

Также проводилась попытка сгенерировать 10000 квазигрупп при $k = 8$, $n = 2$, помещая их в unordered set. Среди сгенерированных квазигрупп оказалось 8944 уникальных объекта. Каждый был проверен на аффинность и простоту. Оказалось, что среди них 8636 были простыми и не было ни одной аффинной. Таким образом, за исключением случая $k = n = 2$ не было обнаружено ни одной аффинной квазигруппы, а подавляющее большинство квазигрупп оказывались простыми.

Аналогичный эксперимент был проведен с сетями Фейстеля. Таблица с результатами:

| $k$ | Всего квазигрупп | Простых | Аффинных |
|---|---|---|---|
| 2 | 4 | 4 | 4 |
| 3 | 36 | 27 | 0 |
| 4 | 576 | 512 | 16 |
| 5 | 14400 | 14250 | 50 |

Как и в предыдущем случае, проводилась попытка сгенерировать 10000 квазигрупп при $k = 8$. Все они оказались уникальными. 9994 из них были простыми и не оказалось ни одной аффиной.

Результаты эксперимента показывают, что оба метода генерации порождают множества, содержащии достаточно большое количество полиномиально полных квазигрупп.

## Проверка наличия подквазигрупп

Наличие подквазигрупп проверялось с использованием алгоритма, описанного в [8]. Таким же образом, как в предыдущем эксперименте, можно получить все квазигруппы нужного порядка. Над каждым полученным объектом проводилось две операции — поиск тривиальных и поиск нетривиальных подквазигрупп. Результаты для регистров сдвига приведены ниже:

| $k$ | $n$ | Всего квазигрупп | Имеющих тривиальные подквазигруппы | Имеющих нетривиальные подквазигруппы |
|---|---|---|---|---|
| 2 | 2 | 2 | 1 | 0 |
| 2 | 3 | 4 | 2 | 0 |
| 2 | 4 | 16 | 8 | 1 |
| 2 | 5 | 256 | 128 | 16 |
| 3 | 2 | 6 | 6 | 0 |
| 3 | 3 | 216 | 216 | 24 |
| 4 | 2 | 24 | 12 | 4 |

Интересным является тот факт, что при $k = 2$ и $k = 4$ в этих экспериментах ровно половина от всех квазигрупп имели подквазигруппу порядка 1. При $k = 3$ в обоих случаях все квазигруппы имели подквазигруппу порядка 1.

Аналогичная таблица для сетей Фейстеля:

| $k$ | Всего квазигрупп | Имеющих тривиальные подквазигруппы | Имеющих нетривиальные подквазигруппы |
|---|---|---|---|
| 2 | 4 | 1 | 0 |
| 3 | 36 | 36 | 9 |
| 4 | 576 | 144 | 16 |
| 5 | 14400 | 14400 | 150 |

Таким образом, по результатам экспериментов кажется, что оба метода генерации порождают множества квазигрупп, в которых не менее четверти квазигрупп имеют подквазигруппы порядка 1. Нетривиальные подквазигруппы имеются у гораздо меньшего количества квазигрупп, а в ряде случаев отсутствуют вовсе.

# 5. Заключение

Рассмотренные классы перестановок с полным дифференциалом оказываются эффективным способом задания квазигрупп. Множества, получаемые таким образом, являются достаточно большими, а алгоритмы генерации позволяют быстро получить случайную квазигруппу из этих множеств. Несмотря на то, что многие такие квазигруппы обладают "неподвижными точками" , этот факт можно учесть при построении криптоалгоритмов. В остальном, подавляющее число получаемых объектов обладают "хорошими" свойстами с точки зрения криптографии.

В дальнейшем, с целью улучшения множеств порождаемых квазигрупп, хочется узнать какими свойствами должны обладать функция $g$ в регистрах сдвига и перестановки $s$ и $p$ в сетях Фейстеля, чтобы порождаемые квазигруппы всегда оказывались полиномиально полными.

# Список литературы

[1] М. М. Глухов, "О применениях квазигрупп в криптографии" , Прикладная дискретная математика, 2008, № 2, 28–32.

[2] Sade, A. 1957. Quasigroups automorphes par le groupe cyclique. Canadian Journal of Mathematics 9:321-335.

[3] J. Hagemann, C. Herrmann, "Arithmetical locally equational classes and representation of partial functions" , Universal Algebra, Esztergom (Hungary), 29 (1982), 345-360.

[4] P.J. Cameron Almost all quasigroups have rank 2. Discrete Mathematics, 1992. Vol. 106-107. P. 111-115.

[5] Личное общение с А.В. Галатенко, А.Е. Панкратьевым и В.А. Носовым

[6] Markovski, S., and A. Mileva. 2009. Generating huge quasigroups from small non-linear bijections via extended Feistel function. Quasigroups and Related Systems 17:97-106.

[7] А.В. Галатенко, А.Е. Панкратьев, "О сложности проверки полиномиальной полноты конечных квазигрупп" , Дискрет. матем., 30:4 (2018), 3-11

[8] Галатенко А.В., Панкратьев А.Е., Староверов В.М. Об одном алгоритме проверки существования подквазигрупп. Чебышевский сборник. 2021;22(2):76-89.