О построении бесформенных полиномиально полных квазигрупп

Д. А. Александров*

В. А. Артамонов, С. Чакрабарти, Ш. К. Тивари и В. Т. Марков в статье «Алгебраические свойства подквазигрупп и построение конечных квазигрупп» предложили метод построения конечных квазигрупп порядка $q = p^r > 4$, где p — простое, $r \in \mathbb{N}$, обеспечивающий полиномиальную полноту и отсутствие собственных подквазигрупп. В работе доказывается, что квазигруппы, полученные с помощью исходной конструкции, не удовлетворяют требованию бесформенности, введенному С. Марковски и Д. Глигороски с соавторами. Предлагается уточнение данной конструкции, позволяющее получать бесформенные квазигруппы, обладающие ранее установленными свойствами.

Ключевые слова: конечные квазигруппы, полиномиальная полнота, бесформенность.

1. Введение

В основе данной работы лежит статья [1], в которой был предложен метод построения конечных квазигрупп порядка $q = p^r > 4$, где p — простое, $r \in \mathbb{N}$, обеспечивающий полиномиальную полноту и отсутствие собственных подквазигрупп. Одна из таких квазигрупп была использована, например, в криптоалгоритме INRU [2]. С. Марковски и Д. Глигороски ввели (см., например, [3]) свойство бесформенности. Мы показали (см. теорему 1 ниже), что не все квазигруппы из работы [1] являются бесформенными.

Обобщение исходной конструкции позволило получить более широкий класс квазигрупп, сохраняющий основные свойства и допускающий наличие бесформенности. Приведен пример для порядка 16, который можно рассматривать как усиление квазигруппы из алгоритма INRU.

2. Основные определения

Определение 1. *Квазигруппой* называется пара $(Q, *)$, где Q — непустое множество, $* : Q \times Q \to Q$ — бинарная операция такая, что для любых

*Александров Демид Андреевич — студент МГУ им. М.В. Ломоносова, e-mail: demid.aleksandrov@math.msu.ru, ORCID: 0009-0007-0576-6039.

Aleksandrov Demid Andreevich — Student, Lomonosov Moscow State University.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

$a, b \in Q$ существуют единственные решения $x, y \in Q$ уравнений $a * x = b$ и $y * a = b$.

В дальнейшем будет предполагаться, что квазигруппы конечные, то есть $|Q| = k < \infty$. Без ограничения общности $Q = E_k = \{0, 1, \ldots, k-1\}$, а квазигрупповая операция — функция k-значной логики.

Определение 2. Пусть задана квазигруппа $(E_k, *)$ и $Q' \subset E_k$, $1 \leq |Q'| < k$. Если для любых элементов $a, b \in Q'$ верно, что $a * b \in Q'$, то будем говорить, что квазигруппа $(E_k, *)$ содержит *собственную подквазигруппу* $(Q', *|_{Q'})$.

Определение 3. Квазигруппа называется *полиномиально полной*, если $\left[\{*\} \cup P_k^0\right] = P_k$, где $[F]$ — стандартным образом определенное замыкание множества функций $F \subseteq P_k$.

Определение 4. Квазигруппа $(E_k, *)$ называется *бесформенной*, если она не идемпотентна, некоммутативна, неассоциативна, не содержит ни левой, ни правой единицы, не содержит собственных подквазигрупп, и не существует $t < 2k$, при котором для всех $x, y \in E_k$ выполняются тождества $\underbrace{x * (x * \ldots * (x}_{t} * y)) = y$ или $(\underbrace{(y * x) * \ldots * x}_{t}) * x = y$.

Рассмотрим конечное поле $\mathbb{F}_k$ $(k = p^r)$ с $k > 4$ элементами, и $\alpha, \beta, c \in \mathbb{F}_k^*$. Пусть $m, d \in \mathbb{N}$ — взаимно простые с $(k-1)$. Определим

$$x * y = \alpha x^m + \beta y^d + c. \tag{1}$$

В статье [1] авторы показали, что операция 1 задает структуру квазигруппы на $\mathbb{F}_k$ и получили следующий результат.

Предположим, что $m \notin \{1, p, \ldots, p^{r-1}\}$, β является порождающим для группы $\mathbb{F}_k^*$, $1 < m < k-1$ взаимно прост с $k-1$ и $d = 1$. Тогда найдется $c \in \mathbb{F}_k^*$, такой что квазигруппа с операцией (1) не имеет собственных подквазигрупп и полиномиально полна [1, Следствие 3.8].

3. Основные результаты

Теорема 1. *Пусть p простое и $k = p^r$. Предположим, что $m \notin \{1, p, \ldots, p^{r-1}\}$, β является порождающим для циклической группы $\mathbb{F}_k^*$, а $1 < m < k-1$ взаимно прост с $(k-1)$ и $d = 1$. Тогда квазигруппа с операцией (1) при $\alpha = 1 - \beta$ неидемпотентна, некоммутативна, неассоциативна, не содержит ни левой, ни правой единицы и удовлетворяет левому тождеству бесформенности при $t = k-1$ и $t = 2k-2$. Существует c, для которого отсутствуют собственные подквазигруппы.*

Теорема 2. *Пусть p простое и $k = p^r$. Предположим, что β является порождающим для циклической группы $\mathbb{F}_k^*$, $md^{-1} \mod (k-1) \notin \{1, p, \ldots, p^{r-1}\}$, а $1 < m, d < k-1$ взаимно просты с $k-1$. Тогда найдется $c \in \mathbb{F}_k^*$ такой, что квазигруппа с умножением $x * y = (1-\beta)x^m + \beta y^d + c$ полиномиально полна и не имеет собственных подквазигрупп.*

Замечание 1. Полиномиальная полнота напрямую следует из [1, следствие 3.4]. Новизна состоит в доказательстве отсутствия подквазигрупп.

С использованием программы https://github.com/Gerror/Quasigroup Р. А. Жигляева, в ходе вычислительных экспериментов удалось найти полиномиально полную, бесформенную квазигруппу порядка 16 (см. таблицу 1), которая может послужить заменой квазигруппы из [2].

Таблица 1: Таблица Кэли для $q = 16$, $m = 13$, $d = 7$, $\beta = 13$, $c = 2$

$*$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	15	4	12	13	8	10	7	1	14	0	6	5	11	3	9
1	14	3	8	0	1	4	6	11	13	2	12	10	9	7	15	5
2	1	12	7	15	14	11	9	4	2	13	3	5	6	8	0	10
3	15	2	9	1	0	5	7	10	12	3	13	11	8	6	14	4
4	6	11	0	8	9	12	14	3	5	10	4	2	1	15	7	13
5	4	9	2	10	11	14	12	1	7	8	6	0	3	13	5	15
6	12	1	10	2	3	6	4	9	15	0	14	8	11	5	13	7
7	0	13	6	14	15	10	8	5	3	12	2	4	7	9	1	11
8	3	14	5	13	12	9	11	6	0	15	1	7	4	10	2	8
9	7	10	1	9	8	13	15	2	4	11	5	3	0	14	6	12
10	10	7	12	4	5	0	2	15	9	6	8	14	13	3	11	1
11	9	4	15	7	6	3	1	12	10	5	11	13	14	0	8	2
12	8	5	14	6	7	2	0	13	11	4	10	12	15	1	9	3
13	5	8	3	11	10	15	13	0	6	9	7	1	2	12	4	14
14	11	6	13	5	4	1	3	14	8	7	9	15	12	2	10	0
15	13	0	11	3	2	7	5	8	14	1	15	9	10	4	12	6

4. Заключение

В работе была рассмотрена и усилена конструкция, введенная в статье [1], позволяющая порождать полиномиально полные квазигруппы без собственных подквазигрупп. Для исходного метода было доказано, что такие квазигруппы не являются бесформенными. Предложено усиление, которое позволяет сохранить полиномиальную полноту и отсутствие собственных подквазигрупп, а также получить бесформенность.

Список литературы

[1] В. А. Артамонов, С. Чакрабарти, Ш. К. Тивари, В. Т. Марков, “Алгебраические свойства подквазигрупп и построение конечных квазигрупп”, *Алгебра и логика*, **61**:4 (2022), 375–400.

[2] S. K. Tiwari, A. Awasthi, S. Chakrabarti, S. Yadav, “INRU: A Quasigroup Based Lightweight Block Cipher”, arXiv: 2112.07411v1.

[3] A. Mileva, S. Markovski, “Shapeless quasigroups derived by Feistel orthomorphisms”, *Glasnik Matematicki*, **47**:2 (2012), 333–349. DOI: 10.3336/gm.47.2.09.

Статья поступила 2 ноября 2026 г.

On the construction of shapeless polynomially complete quasigroups

D. A. Aleksandrov

In their paper “Algebraic Properties of Subquasigroups and Construction of Finite Quasigroups”, V. A. Artamonov, S. Chakrabarti, S. K. Tiwari, and V. T. Markov proposed a method for constructing finite quasigroups of order $q = p^r > 4$, where p is prime and $r \in \mathbb{N}$, that are polynomially complete and have no proper subquasigroups. The paper proves that quasigroups obtained using the original construction do not satisfy the requirement of shaplesness introduced by S. Markovski and D. Gligoroski with co-authors. A refinement of this construction is proposed, which makes it possible to preserve the previously established properties and obtain shapless quasigroups.

Keywords: finite quasigroups, polynomial completeness, shapeless quasigroups.

References

[1] V. A. Artamonov, S. Chakrabarti,Sh. K. Tiwari, V. T. Markov, “Algebraic Properties of Subquasigroups and Construction of Finite Quasigroups”, *Algebra and Logic*, **61**:4 (2022), 251–270. DOI: 10.1007/s10469-023-09695-1.

[2] S. K. Tiwari, A. Awasthi, S. Chakrabarti, S. Yadav, “INRU: A Quasigroup Based Lightweight Block Cipher”, arXiv: 2112.07411v1.

[3] A. Mileva, S. Markovski, “Shapeless quasigroups derived by Feistel orthomorphisms”, *Glasnik Matematicki*, **47**:2 (2012), 333–349. DOI: 10.3336/gm.47.2.09.

Received on November 2, 2026