Об одном критерии полиномиальной полноты квазигрупп

Югай В.Л.

В работе формулируется и доказывается критерий полиномиальной полноты квазигрупп в терминах предполных классов k-значной логики.

Ключевые слова: квазигруппа, полиномиальная полнота, квазилинейность.

1. Введение

В последние годы наблюдается рост интереса к криптосистемам на основе квазигрупп (или, что эквивалентно, на основе латинских квадратов). В качестве примера можно привести работы [1], [2], [3], [4].

С криптографической точки зрения одним из самых важных свойств квазигрупп является полиномиальная полнота. Это обусловлено тем, что в функционально полной алгебре задача распознавания разрешимости системы уравнений является NP-полной ([5]). Известно, что квазигруппа полиномиально полна тогда и только тогда, когда она простая и неаффинная ([6]). Для ряда частных случаев построены более эффективные критерии: в работе [7] рассмотрен случай квазигрупп порядка 4, в работах [8], [9] предложен кубический алгоритм проверки полиномиальной полноты для случая квазигрупп простого порядка. В работе [10] проведено исследование связи свойств простоты и аффинности.

В настоящей работе предлагается критерий полиномиальной полноты, аналогичный критерию из работы [6], но сформулированный в терминах предполных классов k-значной логики.

2. Основные определения

Определение 1. *Квазигруппой* $(Q, *)$ *называется множество элементов* Q *с заданной на нем операцией* $* : Q \times Q \to Q$*, такой что для любых*

$a, b \in Q$ *уравнения*

$$a * x = b$$
$$y * a = b$$

имеют единственное решение.

В дальнейшем мы будем предполагать, что множество Q конечно.

Квазигрупповая операция может быть задана "таблицей умножения" — матрицей M порядка $|Q| \times |Q|$. Занумеруем элементы Q числами от 1 до $|Q|$: $Q = \{q_1, \ldots, q_{|Q|}\}$. Элемент матрицы, стоящий на пересечении строки номер i и столбца номер j, равен $q_i * q_j$. Матрица M называется латинским квадратом, связанным с квазигруппой $(Q, *)$. Несложно увидеть, что каждая строка и каждый столбец M является перестановкой на множестве Q.

Пусть $n \in \mathbb{N} \cup \{0\}$. Обозначим множество всех n-арных операций на множестве Q через P^n. В частности, P^0 — это множество всех констант, являющихся элементами Q. Положим $P = \bigcup\limits_{n=0}^{\infty} P^n$. Заметим, что функции из P можно рассматривать как функции логики значности $|Q|$ и естественным образом ввести операцию замыкания, обозначаемую квадратными скобками: если $F \subseteq P$, то $[F]$ — замыкание F ([11]).

Определение 2. *Квазигруппа $(Q, *)$ называется полиномиально (или функционально) полной, если*

$$\left[\{*\} \cup P^0\right] = P.$$

Определение 3. *Квазигруппа $(Q, *)$ называется простой, если операция $*$ не сохраняет никакое нетривиальтное отношение эквивалентности на множестве Q.*

Несложно увидеть, что все квазигруппы простого порядка являются простыми.

Определение 4. *Квазигруппа $(Q, *)$ называется аффинной, если на множестве Q можно ввести структуру абелевой группы $(Q, +)$, такую что*

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

где α, β — некоторые автоморфизмы группы $(Q, +)$, $c \in Q$.

Известно ([6]), что квазигруппа полиномиально полна тогда и только тогда, когда она проста и неаффинна.

Определение 5. *Функция от n переменных f^n на множестве Q из p^m элементов, где p — простое число, $m \in \mathbb{N}$, называется квазилинейной, если на Q можно ввести структуру конечного поля, относительно которой f^n представима в виде*

$$f^n(x_1, \ldots, x_n) = a_0 + \sum_{i=1}^{n} \sum_{j=0}^{m-1} a_{ij} \cdot x_i^{p^j},$$

В частности, если $m = 1$, такая функция называется линейной.

3. Критерий полиномиальной полноты квазигрупп

Теорема 1. *Квазигруппа $(Q, *)$ полиномиально полна тогда и только тогда, когда операция $*$ не сохраняет никакое нетривиальное отношение эквивалентности на Q и не является квазилинейной.*

Доказательство. Необходимость вытекает из замкнутости и неполноты классов сохранения отношений и классов квазилинейных функций, а также принадлежности всех констант всем таким классам.

Докажем достаточность. Пусть квазигруппа не является полиномиально полной. Тогда она либо не простая, либо аффинная. Если она не простая, то сохраняется нетривиальное отношение эквивалентности.

Пусть квазигруппа простая. Известно ([Предложение 3.2][10]), что простая квазигруппа может быть аффинной, только если порядок является степенью простого числа, а соответствующая абелева группа $(Q, +)$ является примарной. Таким образом, для доказательства достаточности осталось показать, что если квазигруппа аффинна над примарной группой, то квазигрупповая операция квазилинейна.

Пусть $x * y = \alpha(x) + \beta(y) + c$ для некоторой примарной абелевой группы $(Q, +)$, $\alpha, \beta \in Aut((Q, +))$, $c \in Q$. В [Лемма 5.2.4.2][11] показано, что функция $f^n \in P^n$ квазилинейна тогда и только тогда, когда для любых $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in Q^n$ выполнено равенство

$$f^n(a_1 + b_1, \ldots, a_n + b_n) + f(0, \ldots, 0) = f(a_1, \ldots, a_n) + f(b_1, \ldots, b_n),$$

где 0 — нейтральный элемент абелевой группы. Из этого факта вытекает квазилинейность автоморфизмов α и β. Следовательно, и функция $x * y$ квазилинейна. ■

В рамках обозначений предполных классов, принятых в работе [11], теорема может быть переформулирована следующим образом.

Следствие 1. *Квазигруппа* $(Q, *)$ *полиномиально полна тогда и только тогда, когда операция* $*$ *не лежит ни в одном из классов типа* $\mathfrak{U}$ *(сохранения нетривиального отношения эквивалентности) и* $\mathfrak{L}$ *(квазилинейных функций).*

В случае, когда порядок квазигруппы простой, в работах [8], [9] показано, что линейность двухместной функции $x * y$ эквивалентна одновременной линейности функций вида $x * a$ и $b * y$ для всевозможных $a, b \in Q$. В случае, когда порядок является степенью простого числа, это вообще говоря неверно. В качестве примера можно рассмотреть случай $p = m = 2$. В работе [7] показано, что полиномиально полные квазигруппы порядка 4 существуют. В силу доказанного критерия, квазигрупповые операции при этом не квазилинейны. Однако, как несложно увидеть, все 24 перестановки порядка 4 квазилинейны.

Автор выражает глубокую благодарность своему научному руководителю, к.ф.-м.н., с.н.с, А.В. Галатенко за постановку задачи и внимание к работе.

Список литературы

[1] М.М. Глухов. *О применениях квазигрупп в криптографии* // ПДМ, 2008, №2(2), 28–32.

[2] V. Shcherbacov. *Quasigroup based crypto-algorithms* // arXiv:1201.3016.

[3] S. Markovski, D. Gligoroski, V. Bakeva. *Quasigroup String Processing: Part 1* // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci. 1999. Vol. XX, 1–2. P. 13—28.

[4] S. Markovski, V. Kusacatov. *Quasigroup String Processing: Part 2* // Proc. of Maked. Academ. of Sci. and Arts for Math. and Tech. Sci. 2000. Vol. XXI, 1–2. P. 15–32.

[5] G. Horváth, C. L. Nehaniv, Cs. Szabó. *An assertion concerning functionally complete algebras and NP-completeness* // Theoretical Computer Science. 2008. Vol. 407, 1–3. P. 591—595.

[6] J. Hagemann , C. Herrmann. *Arithmetical locally equational classes and representation of partial functions* // Universal Algebra, Esztergom (Hungary), 1982. Vol. 29, Colloq. Math. Soc. Janos Bolyai, P. 345—360.

[7] V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay, S.K. Pal. *On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts* // Quasigroups and Related Systems. 2013. Vol. 21, 2. P. 117—130.

[8] А.В. Галатенко, А.Е. Панкратьев, С.Б. Родин. *О полиномиально полных квазигруппах простого порядка* // Интеллектуальные системы. Теория и приложения. 2016. Т. 20, Вып 3. С. 194—198.

[9] А.В. Галатенко, А.Е. Панкратьев, С.Б. Родин. *О полиномиально полных квазигруппах простого порядка* // Алгебра и логика. Принято к печати.

[10] V.A. Artamonov, S. Chakrabarti, S.K. Pal. *Characterizations of highly non-associative quasigroups and associative triples* // Quasigroups and Related Systems. 2017. Vol. 25, 1. P. 1—19.

[11] D. Lau. *Function algebras on finite sets: a basic course on many-valued logic and clone theory.* Springer, 2006.

A criterion for polynomial completeness of quasigroups

Yugay V.L.

We formulate and prove a criterion for the polynomial completeness of quasigroups in terms of precomplete classes of k-valued logic.

Keywords: quasigroup, polynomial completeness, quasilinearity.