А. В. Галатенко, А. Е. Панкратьев, О сложности проверки полиномиальной полноты конечных квазигрупп, *Дискрет. матем.*, 2018, том 30, выпуск 4, 3–11

DOI: 10.4213/dm1529

Дискретная математика

том 30 выпуск 4 * 2018

УДК 512.548.7+519.716.2 DOI https://doi.org/10.4213/dm1529

О сложности проверки полиномиальной полноты конечных квазигрупп

© 2018 г. А. В. Галатенко*, А. Е. Панкратьев**

В работе исследуется сложность проверки полиномиальной (функциональной) полноты конечных квазигрупп. Показано, что проверка полиномиальной полноты конечной квазигруппы может быть осуществлена за полиномиальное относительно порядка квазигруппы время.

Ключевые слова: квазигруппа, латинский квадрат, полиномиальная полнота

1. Введение

Одним из магистральных направлений развития синтеза современных криптографических примитивов является использование различных алгебраических структур. При этом на смену таким классическим объектам, как кольца вычетов и конечные поля, приходят некоммутативные и даже неассоциативные структуры, среди которых важное место занимают квазигруппы [2].

Для криптографических приложений особый интерес представляют полиномиально (функционально) полные алгебраические структуры, так как проблема распознавания разрешимости системы уравнений в функционально полной алгебре является NP-полной [7]. Как следствие, использование таких структур в качестве платформы обеспечивает более высокую стойкость.

Известно ([6]), что полиномиальная полнота квазигруппы эквивалентна простоте и неаффинности. В [3] это условие переформулировано в терминах предполных классов k-значной логики: квазигруппа не является полиномиально полной тогда и только тогда, когда квазигрупповая операция лежит в одном из классов сохранения нетривиального отношения эквивалентности ($\mathfrak{U}$ в обозначениях книги [9]) или одном из классов квазилинейных функций ($\mathfrak{L}$). Полиномиальная полнота квазигрупп порядка 4 была рассмотрена в [5]. В [1] была предложена кубическая по сложности процедура проверки полиномиальной полноты квазигрупп простого порядка. В [4] было предложено необходимое условие полиномиальной полноты квазигрупп произвольного порядка, кубическое по сложности проверки.

Основным результатом данной работы является полиномиальная процедура проверки полиномиальной полноты конечных квазигрупп произвольного порядка. В

*Место работы: МГУ имени М. В. Ломоносова, e-mail: agalat@msu.ru

**Место работы: МГУ имени М. В. Ломоносова, e-mail: apankrat@intsys.msu.ru

разделе 2 даются основные определения. В разделе 3 изучается процедура проверки простоты квазигруппы. Раздел 4 посвящен выявлению аффинности. Наконец, в разделе 5 результаты о простоте и аффинности суммируются в основной теореме.

Авторы выражают благодарность В.А. Артамонову, В.Т. Маркову и Д.Н. Жуку за полезные обсуждения, а также рецензенту, отметившему ряд неточностей, в частности в доказательстве леммы 3.

2. Основные определения

Все алгебраические структуры, рассматриваемые в настоящей работе, предполагаются конечными.

Определение 1. *Квазигруппой* называется множество Q, на котором определена такая бинарная операция умножения (в дальнейшем обозначаемая символом f_Q или просто f, если из контекста ясно, о какой квазигруппе идет речь), что для любых элементов $a, b \in Q$ уравнения $ax = b$ и $ya = b$ однозначно разрешимы в Q.

Квазигрупповая операция часто задается табличным способом: для множества элементов $\{q_1, \ldots, q_k\}$, составляющих квазигруппу Q, выписывается квадратная таблица размера $k \times k$ (являющаяся, очевидно, латинским квадратом) с окаймляющими строкой и столбцом.

	q_1	$\ldots$	q_k
q_1	a_{11}	$\ldots$	a_{1k}
$\vdots$	$\ldots$	$\ldots$	$\ldots$
q_k	a_{k1}	$\ldots$	a_{kk}

Здесь элемент $a_{ij} \in Q$ — результат применения квазигрупповой операции f к элементам q_i и q_j.

Для фиксированного множества A обозначим через $\mathcal{O}_n(A)$ совокупность всех n-арных операций на A ($n \geqslant 0$) и пусть $\mathcal{O}(A) = \bigcup\limits_n \mathcal{O}_n(A)$.

На произвольном подмножестве $F \subseteq \mathcal{O}(A)$ естественным образом вводятся операции суперпозиции и замыкания (см., например, [9]). Обозначим замыкание множества F через $[F]$.

Определение 2. Квазигруппа Q называется полиномиально (или функционально) полной, если $[\{f_Q\} \cup \mathcal{O}_0(Q)] = \mathcal{O}(Q)$.

Пусть $Q = \{q_1, \ldots, q_k\}$ — некоторое множество, $k \geqslant 2$. Рассмотрим разбиение α множества Q на непересекающиеся подмножества: $Q = A_1 \sqcup \ldots \sqcup A_t$. Будем говорить, что разбиение α нетривиально, если $t > 1$, $A_i \neq \varnothing$, $i = 1, \ldots, t$, и существует такой индекс j, $1 \leqslant j \leqslant t$, что $|A_j| > 1$. Нетривиальное разбиение равномерно, если $|A_1| = |A_2| = \ldots = |A_t|$. Несложно заметить, что принадлежность одному множеству A_i является отношением эквивалентности на множестве Q. Будем использовать запись $a \sim b$ для обозначения принадлежности элементов $a, b \in Q$ одному классу эквивалентности (более точно, следовало бы писать $\overset{\alpha}{\sim}$, однако для простоты обозначений ссылку на разбиение α мы будем опускать).

Рассмотрим бинарную операцию $f\colon Q^2 \to Q$. Говорим, что операция f сохраняет разбиение α, если для любой такой пары наборов $(a_1, a_2), (b_1, b_2) \in Q^2$, что $a_i \sim b_i$, $i = 1, 2$, выполнено $f(a_1, a_2) \sim f(b_1, b_2)$. Легко увидеть, что квазигрупповые операции могут сохранять только равномерные разбиения. Множество операций $F = \{f_1, \ldots, f_t\}$ сохраняет разбиение α, если α сохраняется каждой f_i, $i = 1, \ldots, t$.

Пусть (Q, f) — квазигруппа. Будем говорить, что операция f является простой, если она не сохраняет никакое нетривиальное разбиение Q. В этом случае квазигруппа также называется простой.

Далее, квазигруппа (Q, f) называется аффинной, если на множестве Q можно ввести такую структуру абелевой группы $(Q, +)$, что существуют автоморфизмы α, β группы $(Q, +)$ и элемент $c \in Q$, для которых выполняется тождество

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

При оценке сложности процедур проверки простоты и аффинности квазигруппы элементарными считаются операции чтения и записи в ячейки памяти (в частности, вычисление квазигрупповой операции), а также арифметические операции в $\mathbb{Z}_k$: при $k < 2^{32}$ арифметика реализуется элементарными машинными командами, а для $k > 2^{32}$ необходимые операции длинной модульной арифметики могут быть реализованы с логарифмической (относительно k) сложностью [8].

3. Проверка простоты квазигруппы

Покажем, что проверка простоты квазигруппы может быть проведена со сложностью, полиномиально зависящей от порядка. Сперва сведем проверку сохранения разбиения бинарной операцией к рассмотрению унарных операций.

Лемма 1. *Пусть (Q, f) — некоторая квазигруппа, α — равномерное разбиение множества Q. Операция f сохраняет α тогда и только тогда, когда все унарные операции вида $f(x, a)$ и $f(b, y)$, $a, b \in Q$, сохраняют разбиение α.*

Доказательство. Необходимость является тривиальным следствием рефлексивности отношения эквивалентности, порожденного разбиением α.

Докажем достаточность. Пусть f не сохраняет разбиение α. Следовательно, существует такая пара наборов (a_1, a_2) и (b_1, b_2), что $a_i \sim b_i$, $i = 1, 2$, но $f(a_1, a_2) \not\sim f(b_1, b_2)$. Рассмотрим набор (a_1, b_2). Так как $f(a_1, a_2) \not\sim f(b_1, b_2)$, то выполнено хотя бы одно из условий $f(a_1, a_2) \not\sim f(a_1, b_2)$ и $f(a_1, b_2) \not\sim f(b_1, b_2)$. Если выполнено первое условие, то разбиение α не сохраняется операцией $f(a_1, y)$, если второе условие — операцией $f(x, b_2)$.

Пусть (Q, f) — квазигруппа, $|Q| = k$, $q_i, q_j \in Q$, $q_i \neq q_j$. Рассмотрим следующую процедуру, проверяющую, существует ли сохраняемое f нетривиальное разбиение $\alpha_{i,j}$, в котором $q_i \sim q_j$. Для простоты обозначений множество Q отобразим на начальный отрезок натурального ряда, сопоставив элементу $q_i \in Q$ номер i.

(1) Для каждой неупорядоченной пары t_1, t_2, $1 \leqslant t_1, t_2 \leqslant k$, $t_1 \neq t_2$, будем хранить две метки — эквивалентности и рассмотренности. В начальный момент

времени все пары не эквивалентны и не рассмотрены. Полагаем $i \sim j$, оставшиеся элементы эквивалентны только себе. Помечаем неупорядоченную пару $\{i, j\}$ как эквивалентную.

(2) Рассматриваем произвольную нерассмотренную эквивалентную пару $\{a, b\}$. Для каждой перестановки s вида $f(x, c)$ или $f(d, y)$, $c, d \in Q$, рассматриваем элементы $s(a)$ и $s(b)$. Если эквивалентность $s(a)$ и $s(b)$ еще не установлена, то полагаем $s(a) \sim s(b)$, помечаем эту пару как эквивалентную и выполняем для нее шаг 3. После рассмотрения всех перестановок переходим к шагу 4.

(3) Объединяем классы эквивалентности, которым принадлежат компоненты пары. Помечаем новые эквивалентные пары.

(4) Помечаем пару $\{a, b\}$ как рассмотренную.

(5) Если множество нерассмотренных эквивалентных пар пусто или все элементы попарно эквивалентны, заканчиваем работу, в противном случае переходим к шагу 2.

Лемма 2. *Описанная процедура обладает следующими свойствами.*

(1) *Шаг* 3 *реализует транзитивное замыкание отношения, построенного на шаге* 2.

(2) *Операция* f *сохраняет нетривиальное отношение* α, *относительно которого* $i \sim j$, *тогда и только тогда, когда процедура возвращает нетривиальное разбиение.*

(3) *Сложность однократного выполнения шага* 2 *составляет* $O(k)$.

(4) *Шаги* 2 *и* 3 *будут выполнены не более чем* $\frac{k(k-1)}{2}$ *раз.*

(5) *Общая сложность выполнения шага* 3 *составляет* $O(k^3)$.

Доказательство. Рассмотрим свойство 1. Пусть на шаге 2 возникло отношение ρ, которое после выполнения шага 3 превратилось в отношение ρ'. Транзитивность ρ' следует из того, что множество Q разбито в объединение непересекающихся классов эквивалентных элементов, причем любая пара элементов, эквивалентность которых была установлена на шаге 2, принадлежит одному классу, что означает согласованность с отношением ρ. Предположим, что существует такое транзитивное отношение ρ'', что для любых a и b, $a\rho b$, выполнено $a\rho'' b$, и существуют такие a_0, b_0, что $a_0\rho' b_0$, но неверно, что $a_0\rho'' b_0$. Следовательно, пара $\{a_0, b_0\}$ была добавлена в ρ' в результате объединения классов эквивалентности на шаге 3. Значит, существует такая цепочка $c_1, \ldots, c_t$, что $c_1 = a_0$, $c_t = b_0$, $c_i \rho c_{i+1}$, $i = 1, \ldots, t-1$. Этот факт противоречит транзитивности отношения ρ'', и справедливость свойства 1 доказана.

Рассмотрим свойство 2. Пусть процедура вернула нетривиальное разбиение. В процессе выполнения процедуры для каждой функции вида $f(x, c)$ и $f(d, y)$, $c, d \in Q$, была проверена эквивалентность выходов на каждой паре эквивалентных входов. Следовательно, каждая унарная функция сохраняет восстановленное разбиение, и по лемме 1 восстановленное разбиение сохраняет и операция f.

Пусть процедура вернула тривиальное разбиение, т. е. каждая пара элементов из Q оказалась эквивалентной. Предположим, что существует такое нетривиальное разбиение $\alpha_{i,j}$, $i \neq j$, что $i \overset{\alpha_{i,j}}{\sim} j$, и существуют такие $p, q \in Q$, что $p \overset{\alpha_{i,j}}{\not\sim} q$. Рассмотрим пару $p_0, q_0 \in E_k$, удовлетворяющую следующим условиям:

(а) $p_0 \overset{\alpha_{i,j}}{\not\sim} q_0$,

(b) для всех пар $p', q' \in E_k$, эквивалентность которых была установлена процедурой раньше, чем эквивалентность p_0 и q_0, выполнено $p' \overset{\alpha_{i,j}}{\sim} q'$.

Такая пара существует по предположению. Эквивалентность p_0 и q_0 была установлена либо на шаге 2, либо на шаге 3. В первом случае возникает противоречие с сохранением разбиения $\alpha_{i,j}$ всеми унарными функциями, во втором — с транзитивностью отношения эквивалентности, порождаемого $\alpha_{i,j}$. Таким образом, доказательство свойства 2 завершено.

Рассмотрим свойство 3. Оно следует из того, что общее число унарных функций вида $f(x, c)$ и $f(d, y)$, $c, d \in Q$, равно $2k$, а вычисление значения перестановки и проверка эквивалентности пары чисел может быть реализована за константное время, так как могут быть сведены к обращению к ячейке памяти с заданным адресом.

Рассмотрим свойство 4. На каждой итерации обрабатывается по крайней мере одна нерассмотренная неупорядоченная пара, поэтому число итераций можно оценить сверху числом таких пар, равным $\frac{k(k-1)}{2}$.

Рассмотрим свойство 5. Каждый раз, когда выполняется шаг 3, происходит слияние двух классов, т. е. общее число классов уменьшается по крайней мере на единицу. В начальный момент классов было $k - 1$, в конечный — не меньше одного. Следовательно, выполнение шага 3 происходит не более чем $k - 2$ раз. Однократное выполнение шага 3 сводится к объединению пары классов (эта операция может быть легко реализована за линейное по k время) и пометке новых эквивалентных пар (одна пометка может быть сделана за константное время, а общее число пометок не превосходит общего числа пар, т. е. квадратично по k). Таким образом, общая сложность составляет $O(k^3)$.

Замечание 1. Несложно увидеть, что однократное выполнение шагов 4 и 5 имеет константную сложность.

Из леммы 2 вытекает следующее утверждение.

Теорема 1. *Существует процедура проверки простоты квазигрупповой операции, имеющая сложность, полиномиальную по порядку квазигруппы.*

Доказательство. По лемме 2 сложность проверки того, сохраняется ли разбиение, включающее эквивалентность фиксированной пары элементов, составляет $O\left(k^2 \cdot k + k^3\right) = O\left(k^3\right)$ при $k \to \infty$. Так как все классы имеют равную мощность, достаточно применить процедуру к всевозможным неупорядоченным парам элементов Q вида $\{q_{i_0}, q_j\}$, где индекс i_0 фиксирован, а индекс j принимает произвольные значения, отличные от i_0, т. е. $(k-1)$ раз. Таким образом, общая сложность составит $O\left(k^4\right)$ при $k \to \infty$.

Следствие 1. *Сложность проверки простоты квазигрупповой операции порядка k составляет $O\left(k^4\right)$ при $k \to \infty$.*

Замечание 2. Результаты данного раздела естественным образом могут быть перенесены на случай n-квазигрупп для произвольного $n \in \mathbb{N}$, $n \geqslant 3$. Сложность процедуры останется полиномиальной и составит $O\left(k^{n+2}\right)$ при фиксированном n и $k \to \infty$.

4. Проверка аффинности квазигруппы

Пусть (Q, f) — квазигруппа, $Q = \{q_1, \ldots, q_k\}$, L — латинский квадрат, задающий операцию f. Обозначим перестановку, соответствующую i-й строке L, через σ_i.

Рассмотрим следующую процедуру:

(1) по матрице L строим матрицу L', в которой при каждом $i = 1, \ldots, k$ строка с номером i содержит перестановку $\sigma_i \cdot \sigma_1^{-1}$,

(2) по матрице L' строим матрицу L'', полученную из L' такой перестановкой строк, что первый столбец L'' совпадает с первой строкой; бинарную операцию, порожденную матрицей L'', обозначим через $f_{L''}$,

(3) проверяем, что матрица L'' симметрична (или, что эквивалентно, что операция $f_{L''}$ коммутативна): в случае отсутствия симметричности завершаем процедуру неуспехом,

(4) проверяем ассоциативность $f_{L''}$, т. е. для каждой тройки r, s, t, $1 \leqslant r, s, t \leqslant k$, проверяем равенство

$$f_{L''}\left(f_{L''}(q_r, q_s), q_t\right) = f_{L''}\left(q_r, f_{L''}(q_s, q_t)\right),$$

в случае отсутствия ассоциативности завершаем процедуру неуспехом,

(5) рассматриваем столбец матрицы L, первый элемент которого совпадает с левым верхним элементом L'', обозначаем заданную этим столбцом перестановку через α,

(6) рассматриваем строку матрицы L, первый элемент которой совпадает с левым верхним элементом L'', обозначаем заданную этой строкой перестановку через β,

(7) проверяем, что α и β сохраняют операцию $f_{L''}$, т. е. для любой пары i, j, $1 \leqslant i, j \leqslant k$, выполнены равенства

$$\alpha\left(f_{L''}(q_i, q_j)\right) = f_{L''}\left(\alpha(q_i), \alpha(q_j)\right),$$
$$\beta\left(f_{L''}(q_i, q_j)\right) = f_{L''}\left(\beta(q_i), \beta(q_j)\right),$$

в случае неравенства хотя бы для одной пары завершаем процедуру неуспехом,

(8) обозначаем через c элемент матрицы L, стоящий в левом верхнем углу,

(9) проверяем, что для любой пары i, j, $1 \leqslant i, j \leqslant k$, выполнено равенство

$$f(q_i, q_j) = f_{L''}\left(f_{L''}(\alpha(q_i), \beta(q_j)), c\right),$$

в случае неравенства хотя бы для одной пары завершаем процедуру неуспехом, в противном случае завершаем процедуру успехом.

Покажем, что приведенная процедура решает задачу проверки аффинности квазигруппы (Q, f).

Лемма 3. *Пусть (Q, f) — квазигруппа, аффинная над абелевой группой $(Q, +)$. Тогда для любого $d \in Q$ существует абелева группа $(Q, +')$, для которой элемент d является нейтральным, и (Q, f) аффинна над $(Q, +')$.*

Доказательство. Определим операцию $+'$ по правилу $x +' y = x + y - d$. Пусть $e \in Q$ — нейтральный элемент абелевой группы $(Q, +)$. Рассмотрим отображение $\varphi\colon Q \to Q$, заданное формулой $\varphi(x) = x + d$. Заметим, что $\varphi(x + y) = x + y + d = (x + d) + (y + d) - d = \varphi(x) +' \varphi(y)$. Следовательно, $(Q, +')$ — это абелева группа, изоморфная $(Q, +)$ и имеющая нейтральный элемент $\varphi(e) = d$.

По определению аффинной квазигруппы справедливо тождество $f(x, y) = \alpha'(x) + \beta'(y) + c'$, где α', β' — автоморфизмы $(Q, +)$, $c' \in Q$. Следовательно,

$$f(x, y) = \varphi \circ \varphi^{-1}(\alpha'(x) + \beta'(y) + c') = \varphi(\alpha'(x) + \beta'(y) + c' - d).$$

Заметим, что из определения отображения φ вытекают равенства

$$\alpha'(x) = \alpha \circ \varphi^{-1}(x) + \alpha'(d), \qquad \beta'(y) = \beta \circ \varphi^{-1}(y) + \beta'(d).$$

Поэтому

$$\begin{aligned} f(x, y) &= \varphi(\alpha'(x) + \beta'(y) + c' - d) = \\ &= \varphi\left(\alpha' \circ \varphi^{-1}(x) + \beta' \circ \varphi^{-1}(y) + c' - d + \alpha'(d) + \beta'(d)\right) = \\ &= \varphi \circ \alpha' \circ \varphi^{-1}(x) +' \varphi \circ \beta' \circ \varphi^{-1}(y) +' \varphi\left(c' - d + \alpha'(d) + \beta'(d)\right). \end{aligned}$$

Непосредственной проверкой несложно убедиться в том, что $\varphi \circ \alpha' \circ \varphi^{-1}$ и $\varphi \circ \beta' \circ \varphi^{-1}$ являются автоморфизмами группы $(Q, +')$. Тем самым показано, что квазигруппа (Q, f) аффинна над абелевой группой $(Q, +')$.

Лемма 4. *Процедура возвращает успех в том и только том случае, когда квазигруппа (Q, f) является аффинной.*

Доказательство. Пусть квазигруппа (Q, f) аффинна. Тогда по определению на множестве Q может быть введена структура абелевой группы $(Q, +)$, относительно которой операция f примет вид $f(x, y) = \alpha'(x) + \beta'(y) + c'$, где α', β' — некоторые автоморфизмы $(Q, +)$, $c' \in Q$. В силу леммы 3 без ограничения общности можно считать, что нейтральным элементом группы $(Q, +)$ является левый элемент окаймляющей строки латинского квадрата L. Следовательно перестановки σ_i будут иметь вид $\beta'(y) + c_i$, где c_i попарно различны, а произведения $\sigma_i \cdot \sigma_1^{-1}$ равны $y + c_i'$, где c_1' — нейтральный элемент группы $(Q, +)$, и все c_i' попарно различны. Следовательно, матрица L'' задает таблицу сложения группы $(Q, +)$, т. е. операция $f_{L''}$ коммутативна и ассоциативна, при этом левый верхний элемент является нейтральным по сложению.

В силу аффинности каждый столбец матрицы L имеет вид $\alpha'(x) + w$ для некоторого $w \in Q$. По условию перестановка α переводит нейтральный элемент в нейтральный, т. е. $\alpha = \alpha'$ — автоморфизм группы $(Q, +)$. Аналогичные рассуждения показывают, что $\beta = \beta'$ — автоморфизм $(Q, +)$. Следовательно, операция $f_{L''}$ сохраняется перестановками α и β.

Так как автоморфизмы переводят нейтральный элемент в нейтральный, константа c' совпадает с левым верхним элементом матрицы L, равным c, т. е. процедура успешно восстановила параметры α', β' и c'.

Обратно, пусть процедура вернула представление

$$f(x, y) = f_{L''}\left(f_{L''}(\alpha(x), \beta(y)), c\right).$$

Заметим, что операция $f_{L''}$ получена из f применением перестановок к аргументам, т. е. $(Q, f_{L''})$ — квазигруппа, изотопная (Q, f). В силу условий коммутативности и ассоциативности $f_{L''}$ $(Q, f_{L''})$ является абелевой группой. В силу сохранения операции $f_{L''}$ перестановки α и β являются автоморфизмами $(Q, f_{L''})$. Таким образом, квазигруппа (Q, f) аффинна по определению.

Лемма 5. *Сложность процедуры равна* $O(k^3)$.

Доказательство. Оценим сложность каждого шага процедуры. На первом шаге происходят вычисление обратной перестановки порядка k и k умножений перестановок порядка k. Эти операции могут быть реализованы со сложностью $O(k^2)$.

На втором шаге проводится переупорядочение строк матрицы L'. По первому элементу строки в L' определяется номер строки в L'', т. е. определение номера строки занимает константное время, копирование строки — линейное время, а копирование k строк — квадратичное время.

На третьем шаге проверяется симметричность L'', т. е. проводится $O(k^2)$ сравнений, каждое из которых имеет константную сложность.

На четвертом шаге проводится проверка ассоциативности, т. е. $O(k^3)$ сравнений пар значений, вычисленных с константной сложностью (вычисление операции $f_{L''}(q_i, q_j)$ сводится к чтению элемента матрицы L'' на пересечении строки с номером i и столбца с номером j).

На пятом и шестом шагах проводится поиск перестановок α и β; его несложно реализовать с линейной сложностью.

На седьмом шаге проверяется свойство автоморфизма для перестановок α и β, т. е. равенство в $O(k^2)$ парах, вычисленных с константной сложностью.

Восьмой шаг — вычисление значения c — сводится к чтению левого верхнего элемента L и имеет сложность $O(1)$.

Наконец, на шаге 9 устанавливается справедливость тождества

$$f(x, y) = f_{L''}\left(f_{L''}(\alpha(x), \beta(y)), c\right),$$

т. е. вновь проверяется равенство в $O(k^2)$ парах, вычисленных с константной сложностью.

Таким образом, шаг 4 имеет сложность $O(k^3)$. Сложность же остальных шагов не превосходит $O(k^2)$.

Из лемм 4, 5 непосредственно вытекает следующее утверждение.

Теорема 2. *Проверка аффинности квазигруппы* (Q, f), *заданной латинским квадратом*, *может быть проведена за время*, *полиномиальное по порядку квазигруппы*.

Замечание 3. Результаты раздела естественным образом переносятся на случай n-квазигрупп для произвольного $n > 2$. Сложность процедуры останется полиномиальной и составит $O(k^n)$ при фиксированном n и $k \to \infty$.

5. Проверка полиномиальной полноты квазигруппы

Объединяя теоремы 1 и 2, получаем следующее утверждение.

Теорема 3. *Проверка полиномиальной полноты квазигруппы* (Q, f), *заданной латинским квадратом*, *может быть проведена за время*, *полиномиальное по порядку квазигруппы.*

Замечание 4. В силу равномерности разбиения, сохраняемого квазигрупповой операцией, квазигруппы простого порядка являются простыми, поэтому для установления полиномиальной полноты достаточно проверить аффинность.

Замечание 5. Так как аффинная квазигруппа может быть простой только если ее порядок является степенью простого числа ([4, Proposition 3.2]), то в случае, когда $|Q|$ не представим в виде p^n ни для каких простого p и натурального n, для установления полиномиальной полноты достаточно проверить простоту квазигруппы.

Список литературы

1. А. В. Галатенко, А. Е. Панкратьев, С. Б. Родин, "О полиномиально полных квазигруппах простого порядка", *Алгебра и логика*, принято к печати.
2. М. М. Глухов, "О применениях квазигрупп в криптографии", *Прикладная дискретная математика*, 2008, № 2, 28–32.
3. В. Л. Югай, "Об одном критерии полиномиальной полноты квазигрупп", *Интеллектуальные системы. Теория и приложения*, **21**:3 (2017), 131–135.
4. V. A. Artamonov, S. Chakrabarti, S. K. Pal, "Characterizations of highly non-associative quasigroups and associative triples", *Quasigroups and Related Systems*, **25** (2017), 1–19.
5. 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*, **21** (2013), 117–130.
6. J. Hagemann, C. Herrmann, "Arithmetical locally equational classes and representation of partial functions", *Universal Algebra*, *Esztergom* (*Hungary*), **29** (1982), 345–360.
7. G. Horváth, Gh. L. Nehaniv, Cs. Szabó, "An assertion concerning functionally complete algebras and NP-completeness", *Acta Sci. Math.* (*Szeged*), **76** (2010), 35–48.
8. Кнут Д.Э., *Искусство программирования. Том* 2, 3-е издание, Вильямс, 2001; пер. с англ.: D. Knuth, *The Art of Computer Programming*, v. 2: *Seminumerical Algorithms*, 3, Addison-Wesley, 2008.
9. D. Lau, *Function algebras on finite sets*: *a basic course on many-valued logic and clone theory*, Springer, 2006.

Статья поступила 25.05.2018.
Переработанный вариант поступил 12.10.2018.