Математические заметки

Том 96 выпуск 6 декабрь 2014

УДК 512.643

$p(x)$-циркулянты над конечными полями и вероятностные методы их построения

В. В. Гриценко, А. Э. Маевский

В статье изучается алгебра $p(x)$-циркулянтов над произвольным конечным полем и строятся алгоритмы случайного равновероятного выбора элементов из подмножества всех обратимых $p(x)$-циркулянтов или подмножества всех $p(x)$-циркулянтов с заданным значением определителя. Особенностью рассматриваемых алгоритмов является минимизация временной сложности и количества случайных элементов, используемых в процессе их работы.

Библиография: 13 названий.

DOI: 10.4213/mzm10385

1. Введение. Пусть $\mathbb{F}_q$, $q=p^s$, $s\in\mathbb{N}$, – конечное поле из q элементов характеристики p, $\mathbb{F}_q[x]$ – кольцо многочленов одной переменной x над полем $\mathbb{F}_q$. Зафиксируем натуральное число n (>1) и многочлен $p(x)\in\mathbb{F}_q[x]$ вида

$$p(x)=x^n-p_{n-1}x^{n-1}-\dots-p_1x-p_0.$$

Матрицу $n\times n$ над полем $\mathbb{F}_q$, построенную по вектору $\mathbf{c}=(c_0,\dots,c_{n-1})$ из $\mathbb{F}_q^n$ следующим образом:

$$\begin{pmatrix} c_1^{(1)}\triangleq c_0 & c_1^{(2)}\triangleq c_n^{(1)}p_0 & \cdots & c_1^{(n)}\triangleq c_n^{(n-1)}p_0\\ c_2^{(1)}\triangleq c_1 & c_2^{(2)}\triangleq c_n^{(1)}p_1+c_1^{(1)} & \cdots & c_2^{(n)}\triangleq c_n^{(n-1)}p_1+c_1^{(n-1)}\\ c_3^{(1)}\triangleq c_2 & c_3^{(2)}\triangleq c_n^{(1)}p_2+c_2^{(1)} & \cdots & c_3^{(n)}\triangleq c_n^{(n-1)}p_2+c_2^{(n-1)}\\ \vdots & \vdots & \ddots & \vdots\\ c_n^{(1)}\triangleq c_{n-1} & c_n^{(2)}\triangleq c_n^{(1)}p_{n-1}+c_{n-1}^{(1)} & \cdots & c_n^{(n)}\triangleq c_n^{(n-1)}p_{n-1}+c_{n-1}^{(n-1)}\end{pmatrix},$$

будем называть $p(x)$-*циркулянтом* над полем $\mathbb{F}_q$ и обозначать $M_{p(x)}(\mathbf{c})$. Отметим, что определение $p(x)$-циркулянта расширяет и обобщает различные типы циркулянтов, рассматриваемых ранее при решении фундаментальных и прикладных задач.

Работа второго автора выполнена при поддержке Российского фонда фундаментальных исследований (грант № 13-07-00978).

© В. В. Гриценко, А. Э. Маевский, 2014

Так, произвольный (x^n-1)-циркулянт имеет вид

$$M_{x^n-1}(\mathbf{c})=\begin{pmatrix} c_0 & c_{n-1} & c_{n-2} & \dots & c_2 & c_1 \\ c_1 & c_0 & c_{n-1} & \dots & c_3 & c_2 \\ c_2 & c_1 & c_0 & \dots & c_4 & c_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{n-1} & c_{n-2} & c_{n-3} & \dots & c_1 & c_0 \end{pmatrix}$$

традиционного циркулянта, построенного по первому столбцу, (x^n-r)-циркулянт имеет вид

$$M_{x^n-r}(\mathbf{c})=\begin{pmatrix} c_0 & rc_{n-1} & rc_{n-2} & \dots & rc_2 & rc_1 \\ c_1 & c_0 & rc_{n-1} & \dots & rc_3 & rc_2 \\ c_2 & c_1 & c_0 & \dots & rc_4 & rc_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{n-2} & c_{n-3} & c_{n-4} & \dots & c_0 & rc_{n-1} \\ c_{n-1} & c_{n-2} & c_{n-3} & \dots & c_1 & c_0 \end{pmatrix}$$

r-косоциркулянта [1; с. 47], а произвольный (x^n-x-r)-циркулянт имеет вид

$$M_{x^n-x-r}(\mathbf{c})=\begin{pmatrix} c_0 & rc_{n-1} & rc_{n-2} & \dots & rc_2 & rc_1 \\ c_1 & c_0+c_{n-1} & rc_{n-1}+c_{n-2} & \dots & rc_3+c_2 & rc_2+c_1 \\ c_2 & c_1 & c_0+c_{n-1} & \dots & rc_4+c_3 & rc_3+c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{n-2} & c_{n-3} & c_{n-4} & \dots & c_0+c_{n-1} & rc_{n-1}+c_{n-2} \\ c_{n-1} & c_{n-2} & c_{n-3} & \dots & c_1 & c_0+c_{n-1} \end{pmatrix}$$

FLS-r-циркулянта [2]. Множество всех $p(x)$-циркулянтов над полем $\mathbb{F}_q$ обозначим $GCR_{p(x)}$. Целью настоящей работы является исследование алгебраической структуры множества $GCR_{p(x)}$ и разработка эффективных алгоритмов случайного равновероятного выбора его элементов, обладающих некоторыми заданными свойствами.

Широко известно (например, [3; с. 484]), что множество GCR_{x^n-1} является коммутативной $\mathbb{F}_q$-алгеброй с обычными операциями сложения и умножения матриц. Распространение этого утверждения на случай $p(x)$-циркулянтов над произвольным полем, где $p(x)$ – сепарабельный многочлен, получено в работе [4]. В настоящей статье в п. 2 аналогичный факт устанавливается для множества $GCR_{p(x)}$ при произвольно заданном многочлене $p(x)\in\mathbb{F}_q[x]$ без каких-либо ограничений, изучается структура алгебры $GCR_{p(x)}$, обосновывается вычислительно эффективный критерий обратимости элементов $GCR_{p(x)}$ вместе со способом построения обратных элементов, а также приводится формула вычисления определителя произвольного $p(x)$-циркулянта. В пп. 3, 4 статьи решается обратная задача построения вычислительно эффективных алгоритмов случайного равновероятного выбора из множества обратимых $p(x)$-циркулянтов (п. 3) или из множества всех $p(x)$-циркулянтов с заданным значением определителя (п. 4). Под вычислительной эффективностью алгоритмов при этом понимается минимизация вычислительной сложности и количества используемых при работе случайных элементов.

Результаты работы могут быть использованы в различных областях математики, где возникают циркулянты, их обобщения или случайные матрицы над конечными

полями – например, при построении новых методов цифровой обработки сигналов и защиты информации, или при реализации (модификации) уже существующих. Так, в теории помехоустойчивого кодирования изучаются циклические или обобщенные циклические (псевдоциклические) коды [3; гл. 7, 8], элементы которых тесно связаны с $p(x)$-циркулянтами [4], а в работе [5] исследуется сложность задачи дискретного логарифмирования в группе обратимых циркулянтов и строится аналог криптосистемы Эль-Гамаля. Случайные обратимые матрицы над конечными полями требуются, например, в криптосистеме Мак-Элиса [6] и ее многочисленных обобщениях, рюкзачной криптосистеме Шамира, при построении моделей защиты информации от частичного перехвата [7], [8].

Всюду далее будем придерживаться следующих соглашений. Все рассматриваемые в статье алгебры считаются определенными над полем $\mathbb{F}_q$, ассоциативными и обладающими единичным элементом. Если W – конечномерная алгебра, то через W^* обозначается множество всех ее обратимых элементов. Через $\mathbb{Z}$ обозначим множество всех целых чисел,

$$[a,b] \triangleq \{x \in \mathbb{Z} \mid a \leqslant x \leqslant b\}.$$

Для произвольного натурального q определим множество

$$\mathbb{Z}_q \triangleq [0, q-1]$$

вместе с операциями сложения и умножения элементов по модулю q.

2. Алгебраическая структура множества $GCR_{p(x)}$. Рассмотрим фактор-кольцо $B_{p(x)} = \mathbb{F}_q[x]/(p(x))$ как $\mathbb{F}_q$-алгебру и в каждом классе эквивалентности зафиксируем представителя – многочлен наименьшей степени. Всюду далее элементы $B_{p(x)}$ отождествляются с их представителями. Ясно, что алгебра $B_{p(x)}$ ассоциативна, коммутативна и обладает единицей. Отметим, что $\dim_{\mathbb{F}_q} B_{p(x)} = n$.

Через $M_n(\mathbb{F}_q)$ обозначим полную матричную алгебру, состоящую из всех матриц размера $n \times n$ над полем $\mathbb{F}_q$.

Теорема 1. *Множество $GCR_{p(x)} \subset M_n(\mathbb{F}_q)$ является коммутативной подалгеброй с единицей, изоморфной алгебре $B_{p(x)}$.*

Доказательство. Покажем, что множество $GCR_{p(x)}$ совпадает с образом некоторого точного матричного представления алгебры $B_{p(x)}$.

Пусть $\mathscr{L}(B_{p(x)})$ – алгебра всех $\mathbb{F}_q$-линейных операторов, действующих на алгебре $B_{p(x)}$, рассматриваемой как конечномерное векторное пространство размерности n $(= \deg p(x))$. Пусть $\mathcal{X} \in \mathscr{L}(B_{p(x)})$ – линейный оператор, действующий по формуле

$$\forall\, a(x) \in B_{p(x)} \qquad \mathcal{X}(a(x)) = x \cdot a(x).$$

Так как алгебра $B_{p(x)}$ порождена элементом x, то сопоставление элементу x оператора $\mathcal{X}$ можно единственным образом продолжить до гомоморфизма φ алгебр $B_{p(x)}$ и $\mathscr{L}(B_{p(x)})$, сохраняющего единичный элемент. По построению φ является регулярным представлением алгебры $B_{p(x)}$.

Покажем, что φ точно. Любому ненулевому элементу $f(x) \in B_{p(x)}$ гомоморфизм φ сопоставляет оператор $f(\mathcal{X})$, действующий на алгебре $B_{p(x)}$ следующим образом:

$$\forall\, a(x) \in B_{p(x)} \qquad f(\mathcal{X})(a(x)) = f(x) \cdot a(x).$$

В частности, $f(\mathcal{X})(1) = f(x)$, поэтому никакой ненулевой элемент $B_{p(x)}$ не соответствует нулевому оператору $\mathscr{L}(B_{p(x)})$ и $\ker\varphi = \{0\}$.

В алгебре $B_{p(x)}$ зафиксируем базис $e = \{1, x, x^2, \dots, x^{n-1}\}$ и через ε_e обозначим соответствующий изоморфизм $\mathscr{L}(B_{p(x)})$ и $M_n(\mathbb{F}_q)$. Тогда $\varepsilon_e \circ \varphi$ – точное матричное представление алгебры $B_{p(x)}$, при котором произвольному элементу

$$f(x) = f_0 + f_1 x + \dots + f_{n-1}x^{n-1} \in B_{p(x)}$$

соответствует матрица оператора $f(\mathcal{X})$ в базисе e, имеющая, как нетрудно проверить прямыми вычислениями, вид $M_{p(x)}(\mathbf{f})$, где $\mathbf{f} = (f_0, f_1, \dots, f_{n-1})$. Следовательно,

$$\operatorname{Im}(\varepsilon_e \circ \varphi) \subseteq GCR_{p(x)},$$

но $\dim_{\mathbb{F}_q} B_{p(x)} = n$ и $|GCR_{p(x)}| = q^n$, поэтому

$$\operatorname{Im}(\varepsilon_e \circ \varphi) = GCR_{p(x)}.$$

В ходе доказательства теоремы 1 каждому $p(x)$-циркулянту

$$M_{p(x)}(\mathbf{c}), \qquad \mathbf{c} = (c_0, c_1, \dots, c_{n-1}),$$

взаимно однозначно сопоставляется многочлен

$$c(x) = c_0 + c_1 x + \dots + c_{n-1}x^{n-1}$$

из алгебры $B_{p(x)}$. Отметим, что степень многочлена $c(x)$ может быть меньше $n-1$. Многочлен $c(x)$ будем называть *определяющим многочленом* для $p(x)$-циркулянта $(\varepsilon_e \circ \varphi)(c(x)) = M_{p(x)}(\mathbf{c})$.

Изоморфизм алгебр $GCR_{p(x)}$ и $B_{p(x)}$ позволяет применить известные методы и результаты исследования структуры алгебры $B_{p(x)}$ к алгебре $GCR_{p(x)}$. Для замкнутости изложения материала приведем некоторые из них.

Лемма 1. *Пусть в кольце $\mathbb{F}_q[x]$ многочлен $p(x)$ раскладывается в произведение степеней неприводимых многочленов следующим образом*:

$$p(x) = p_1^{s_1}(x)p_2^{s_2}(x)\cdots p_t^{s_t}(x). \tag{2.1}$$

Тогда

(i) $GCR_{p(x)} \cong B_{p_1^{s_1}(x)} \oplus B_{p_2^{s_2}(x)} \oplus \dots \oplus B_{p_t^{s_t}(x)}$;

(ii) $GCR^*_{p(x)} \cong (B_{p_1^{s_1}(x)})^* \oplus (B_{p_2^{s_2}(x)})^* \oplus \dots \oplus (B_{p_t^{s_t}(x)})^*$;

(iii) *алгебра $GCR_{p(x)}$ не содержит ненулевых нильпотентных элементов (полупроста) тогда и только тогда, когда $s_1 = s_2 = \dots = s_t = 1$.*

Доказательство. Широко известно, что $B_{p(x)}$ – кольцо главных идеалов. Утверждения (i) и (ii) следуют из теоремы 1 и китайской теоремы об остатках для коммутативных колец главных идеалов. Для доказательства утверждения (iii) заметим, что нильрадикал $\operatorname{rad}(GCR_{p(x)})$ алгебры $GCR_{p(x)}$ есть главный идеал, порожденный $p(x)$-циркулянтом $M_{p(x)}(\mathbf{r})$, где

$$\mathbf{r} = (\varepsilon_e \circ \varphi)(p_1(x)p_2(x)\cdots p_t(x)).$$

Действительно, все простые ненулевые идеалы алгебры $B_{p(x)}$ максимальны, нильрадикал совпадает с радикалом Джекобсона и может быть определен как пересечение всех максимальных идеалов алгебры $B_{p(x)}$. Легко проверяется, что множество всех максимальных идеалов (максимальный спектр) алгебры $B_{p(x)}$ имеет вид

$$\mathrm{Specm}(B_{p(x)}) = \{(p_1(x)), (p_2(x)), \dots, (p_t(x))\}.$$

Так как все многочлены $p_1(x), \dots, p_t(x)$ неприводимы, то и попарно взаимно просты. Следовательно,

$$\bigcap_{i=1}^{t}(p_i(x)) = (\text{НОК}\{p_1(x), p_2(x), \dots, p_t(x)\}) = p_1(x)p_2(x)\cdots p_t(x).$$

Следующая лемма доставляет критерий обратимости и формулу обратного элемента для произвольного $p(x)$-циркулянта.

Лемма 2. *$p(x)$-Циркулянт $M_{p(x)}(\mathbf{c})$ обратим в алгебре $M_n(\mathbb{F}_q)$ тогда и только тогда, когда определяющий его многочлен $c(x)$ взаимно прост с многочленом $p(x)$ (в кольце $\mathbb{F}_q[x]$). При этом обратная матрица к $M_{p(x)}(\mathbf{c})$ также является $p(x)$-циркулянтом с определяющим многочленом $(c(x))^{-1} \pmod{p(x)}$.*

Доказательство. Так как алгебра $M_n(\mathbb{F}_q)$ конечномерна, то любой ее элемент является либо делителем нуля, либо обратим. Следовательно, любая подалгебра $W \subset M_n(\mathbb{F}_q)$ наполнена в $M_n(\mathbb{F}_q)$ ($W^* = M_n(\mathbb{F}_q)^* \cap W$). В частности, если $p(x)$-циркулянт $M_{p(x)}(\mathbf{c})$ обратим, то обратная матрица также является $p(x)$-циркулянтом с некоторым определяющим многочленом $\widetilde{c}(x)$. В силу изоморфизма алгебр $GCR_{p(x)}$ и $B_{p(x)}$ должно выполняться сравнение

$$c(x)\widetilde{c}(x) \equiv 1 \pmod{p(x)}.$$

Утверждение леммы теперь следует из широко известного критерия обратимости элементов кольца $B_{p(x)}$.

Следствие 1. *Всякий ненулевой $p(x)$-циркулянт обратим (алгебра $B_{p(x)}$ проста и является конечным алгебраическим расширением поля $\mathbb{F}_q$) тогда и только тогда, когда многочлен $p(x)$ неприводим как элемент кольца $\mathbb{F}_q[x]$.*

Напомним, что для всякого конечного алгебраического расширения $\mathbb{F}_{q^n}$ поля $\mathbb{F}_q$ некоторой степени n определена мультипликативная функция

$$N\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, \qquad N(\alpha) = \prod_{i=0}^{n-1} \alpha^{q^i},$$

называемая *нормой*. Известно [9; с. 77], что образ нормы совпадает с образом поля $\mathbb{F}_q$ относительно естественного вложения $\mathbb{F}_q$ в $\mathbb{F}_{q^n}$. В силу этого будем считать, что норма сопоставляет каждому элементу $\mathbb{F}_{q^n}$ элемент из $\mathbb{F}_q$. В случае, когда $B_{p(x)}$ – поле, соответствующую функцию нормы из $B_{p(x)}$ в $\mathbb{F}_q$ будем обозначать $N_{p(x)}$.

Лемма 3. *Пусть в кольце $\mathbb{F}_q[x]$ для многочлена $p(x)$ имеет место разложение вида (2.1). Тогда для любого $p(x)$-циркулянта $M_{p(x)}(\mathbf{c})$ с определяющим многочленом $c(x)$ имеем*

$$\det M_{p(x)}(\mathbf{c}) = \prod_{i=1}^{t} (N_{p_i(x)}(c_i(x)))^{s_i}, \tag{2.2}$$

где $c_i(x)$ – остаток от деления $c(x)$ на $p_i(x)$, рассматриваемый как элемент $B_{p_i(x)}$, а произведение вычисляется в поле $\mathbb{F}_q$.

Доказательство утверждения леммы проведем в несколько этапов.

(i) Рассмотрим случай, когда в разложении (2.1) $t = 1$ и $s_1 = 1$. Тогда многочлен $p(x)$ неприводим в $\mathbb{F}_q[x]$ и алгебра $B_{p(x)}$ – поле. Пусть $a(x) \in B_{p(x)}$ – произвольно выбранный примитивный элемент $B_{p(x)}$, порождающий мультипликативную группу $(B_{p(x)})^*$, $m_{a(x)}(t) \in \mathbb{F}_q[t]$ – его минимальный многочлен. Известно [9; гл. 2, § 3], что

$$\deg m_{a(x)}(t) = \deg p(x) = n, \qquad N_{p(x)}(a(x)) = (-1)^n m_0,$$

где m_0 – свободный коэффициент многочлена $m_{a(x)}(t)$. В силу изоморфизма алгебр $B_{p(x)}$ и $GCR_{p(x)}$ многочлен $m_{a(x)}(t)$ совпадает с минимальным многочленом соответствующего $p(x)$-циркулянта $M_{p(x)}(\mathbf{a}) = (\varepsilon_e \circ \varphi)(a(x))$ и, так как $\deg m_{a(x)}(t) = n$, с характеристическим многочленом $M_{p(x)}(\mathbf{a})$. Поскольку определитель матрицы совпадает с точностью до знака со свободным коэффициентом ее характеристического многочлена, имеем

$$\det M_{p(x)}(\mathbf{a}) = N_{p(x)}(a(x)).$$

Так как $a(x)$ – примитивный элемент $B_{p(x)}$, то для произвольного ненулевого $c(x) \in B_{p(x)}$ существует такое $i \in [0, q^n - 1]$, что $c(x) = (a(x))^i$. Тогда

$$M_{p(x)}(\mathbf{c}) = (\varepsilon_e \circ \varphi)(c(x)) = (\varepsilon_e \circ \varphi)((a(x))^i) = ((\varepsilon_e \circ \varphi)(a(x)))^i = (M_{p(x)}(\mathbf{a}))^i,$$
$$\det M_{p(x)}(\mathbf{c}) = (\det M_{p(x)}(\mathbf{a}))^i = (N_{p(x)}(a(x)))^i = N_{p(x)}((a(x))^i) = N_{p(x)}(c(x)).$$

Последнее равенство выполняется в силу мультипликативности функции нормы. Для завершения доказательства леммы в рассматриваемом случае заметим, что нулевому элементу $B_{p(x)}$ соответствует нулевой $p(x)$-циркулянт и $N_{p(x)}(0) = 0$.

(ii) Пусть $p(x) = p_1^{s_1}(x)$, $s_1 > 1$, $p_1(x)$ – неприводимый многочлен в $\mathbb{F}_q[x]$ степени n_1. Алгебру $B_{p(x)}$ рассмотрим как векторное пространство над полем $\mathbb{F}_q$ размерности $n = n_1 s_1$ и зафиксируем множество

$$\mathcal{F} = \{1, x, x^2, \dots, x^{n_1-1}, p_1(x), xp_1(x), \dots, x^{n_1-1}p_1(x),$$
$$p_1^2(x), \dots, p_1^{s_1-1}(x), \dots, x^{n_1-1}p_1^{s_1-1}(x)\}.$$

Так как все степени многочленов из $\mathcal{F}$ различны и пробегают все множество $[0, n-1]$, то $\mathcal{F}$ – базис $B_{p(x)}$. Как и при доказательстве теоремы 1 через $\varepsilon_{\mathcal{F}}$ обозначим изоморфизм $\mathscr{L}(B_{p(x)})$ и $M_n(\mathbb{F}_q)$, сопоставляющий оператору из $\mathscr{L}(B_{p(x)})$ его матрицу в базисе $\mathcal{F}$. Ясно, что $\varepsilon_{\mathcal{F}} \circ \varphi$ – точное матричное представление $B_{p(x)}$, изоморфное представлению $\varepsilon_e \circ \varphi$ (изоморфизм осуществляется с помощью матриц перехода между базисами e и $\mathcal{F}$). Следовательно,

$$\forall\, c(x) \in B_{p(x)} \qquad \det(\varepsilon_e \circ \varphi)(c(x)) = \det(\varepsilon_{\mathcal{F}} \circ \varphi)(c(x)).$$

Прямыми вычислениями проверяется, что

$$(\varepsilon_{\mathcal{F}} \circ \varphi)(x) = \begin{pmatrix} R & O & O & \dots & O & O \\ S & R & O & \dots & O & O \\ O & S & R & \dots & O & O \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ O & O & O & \dots & S & R \end{pmatrix},$$

где R – матрица размера $n_1 \times n_1$, совпадающая с $p_1(x)$-циркулянтом $M_{p_1(x)}(\mathbf{c})$, $\mathbf{c} = (0, 1, 0, \dots, 0)$, порождающим алгебру $B_{p_1(x)}$, S – элементарная квадратная матрица размера $n_1 \times n_1$ с единичным элементом в верхнем правом углу, O – нулевая матрица размера $n_1 \times n_1$. Так как элемент x порождает алгебру $B_{p(x)}$, то для всякого $c(x)$ из $B_{p(x)}$:

$$(\varepsilon_{\mathcal{F}} \circ \varphi)(c(x)) = \varepsilon_{\mathcal{F}}(c(\mathcal{X})) = c(\varepsilon_{\mathcal{F}}(\mathcal{X})) = \begin{pmatrix} c(R) & O & \dots & O & O \\ * & c(R) & \dots & O & O \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ * & * & \dots & * & c(R) \end{pmatrix}.$$

Заметим, что $c(R)$ также является $p_1(x)$-циркулянтом и, так как минимальный многочлен R совпадает с $p_1(x)$, $c(R) = c_1(R)$, где $c_1(x)$ – остаток от деления $c(x)$ на $p_1(x)$ (как многочленов из кольца $\mathbb{F}_q[x]$). Тогда определитель квазинижнетреугольной матрицы $(\varepsilon_{\mathcal{F}} \circ \varphi)(c(x))$ [10; с. 57] есть

$$\det(\varepsilon_{\mathcal{F}} \circ \varphi)(c(x)) = (\det c_1(R))^{s_1} = (N_{p_1(x)}(c_1(x))^{s_1}.$$

Последнее равенство верно в силу доказательства случая (i) и завершает доказательство случая (ii).

(iii) Пусть для многочлена $p(x)$ выполняется разложение вида (2.1) и $t > 1$. Для каждого $i \in [1, t]$ определим линейное представление

$$\rho_i \colon B_{p(x)} \to \mathscr{L}(B_{p_i^{s_i}}(x)), \qquad c(x) \mapsto c(\mathcal{X}),$$

и рассмотрим сумму представлений

$$\rho = \rho_1 + \dots + \rho_t \colon B_{p(x)} \to \mathscr{L}(B_{p_1^{s_1}(x)} \oplus \dots \oplus B_{p_t^{s_t}(x)}),$$

определяемую формулой

$$\forall c(x) \in B_{p(x)} \qquad \rho(c(x))(a_1(x), \dots, a_t(x)) = (c(x) \cdot a_1(x), \dots, c(x) \cdot a_t(x)).$$

Ясно, что ρ – линейное представление, изоморфное регулярному представлению φ. Действительно, гомоморфизм

$$\lambda \colon B_{p(x)} \to B_{p_1^{s_1}(x)} \oplus \dots \oplus B_{p_t^{s_t}(x)}, \quad a(x) \mapsto (a(x) \pmod{p_1^{s_1}(x)}, \dots, a(x) \pmod{p_t^{s_t}(x)})$$

в соответствии с китайской теоремой об остатках является изоморфизмом и, как нетрудно убедиться, для произвольного $c(x) \in B_{p(x)}$ следующая диаграмма коммутативна:

$$\begin{tikzcd} B_{p(x)} \arrow[r, "\varphi(c(x))"] \arrow[d, "\lambda"'] & B_{p(x)} \arrow[d, "\lambda"] \\ B_{p_1^{s_1}(x)} \oplus \dots \oplus B_{p_t^{s_t}(x)} \arrow[r, "\rho(c(x))"] & B_{p_1^{s_1}(x)} \oplus \dots \oplus B_{p_t^{s_t}(x)} \end{tikzcd}$$

Как следствие, в алгебре $B_{p(x)}$ можно зафиксировать такой базис $\mathcal{G}$ и соответствующий ему изоморфизм $\varepsilon_{\mathcal{G}}$ алгебр $\mathscr{L}(B_{p(x)})$ и $M_n(\mathbb{F}_q)$, что

$$\forall\, c(x) \in B_{p(x)} \qquad (\varepsilon_{\mathcal{G}} \circ \varphi)(c(x)) = \begin{pmatrix} c_1(R_1) & O & \dots & O & O \\ O & c_2(R_2) & \dots & O & O \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ O & O & \dots & O & c_t(R_t) \end{pmatrix},$$

где R_i – матрица размера $s_i \deg(p_i(x)) \times s_i \deg(p_i(x))$, совпадающая с $p_i^{s_i}(x)$-циркулянтом $M_{p_i^{s_i}(x)}((0,1,0,\dots,0))$, порождающим алгебру $B_{p_i^{s_i}(x)}$, $(c_1(x),\dots,c_t(x)) = \lambda(c(x))$. В силу изоморфизма матричных представлений $\varepsilon_e \circ \varphi$ и $\varepsilon_{\mathcal{G}} \circ \varphi$ для произвольного $c(x)$ из $B_{p(x)}$ имеем

$$\det(\varepsilon_e \circ \varphi)(c(x)) = \det(\varepsilon_{\mathcal{G}} \circ \varphi)(c(x)) = \prod_{i=1}^{t} \det c_i(R_i),$$

что с применением случая (ii) завершает доказательство леммы.

Через $(\mathbb{F}_q^*)^m$ обозначим образ эндоморфизма возведения в натуральную степень m мультипликативной группы конечного поля $\mathbb{F}_q$.

Следствие 2. *Пусть имеет место* (2.1) *и* $m = \text{НОД}(s_1, s_2, \dots, s_t, q-1)$. *Тогда образ отображения*

$$\det\colon GCR_{p(x)} \to \mathbb{F}_q,$$

сопоставляющего $p(x)$*-циркулянту значение его определителя, равен* $(\mathbb{F}_q^*)^m \cup \{0\}$.

Доказательство. В соответствии с (2.2)

$$\forall\, M_{p(x)}(\mathbf{c}) \in GCR_{p(x)} \qquad \det M_{p(x)}(\mathbf{c}) = a_1 a_2 \cdots a_t, \tag{2.3}$$

где

$$a_i = (N_{p_i(x)}(c_i(x)))^{s_i} \in (\mathbb{F}_q^*)^{s_i} \cup \{0\}, \qquad i \in [1,t].$$

Ясно, что $\det M_{p(x)}(\mathbf{c}) = 0$ тогда и только тогда, когда в (2.3) найдется $a_i = 0$. Пусть $\det M_{p(x)}(\mathbf{c}) \neq 0$, α – примитивный элемент поля $\mathbb{F}_q$, m_i $(i \in [1,t])$, – такие элементы $\mathbb{Z}_{q-1}$, что $a_i = (\alpha^{m_i})^{s_i}$. Тогда

$$\prod_{i\in[1,t]} a_i = \prod_{i\in[1,t]} (\alpha^{m_i})^{s_i} = \alpha^M, \qquad M = \sum_{i\in[1,t]} m_i s_i \in (s_1) + \dots + (s_t) = (r) \subseteq \mathbb{Z}_{q-1},$$

где $r = \text{НОД}(s_1, s_2, \dots, s_t)$. В силу сюръективности $N_{p(x)}$ для всех неприводимых $p(x) \in \mathbb{F}_q[x]$ [9; с. 77] каждый элемент идеала (r) имеет прообраз относительно отображения det. Но

$$(r) = (s_1) + \dots + (s_t) = (s_1) + \dots + (s_t) + (q-1) = (m)$$

в $\mathbb{Z}_{q-1}$, откуда

$$\det M_{p(x)}(\mathbf{c}) = \alpha^M = (\alpha^u)^m \in (\mathbb{F}_q^*)^m$$

для некоторого $u \in \mathbb{Z}_{q-1}$.

3. Алгоритм построения обратимых $p(x)$-циркулянтов. Рассмотрим задачу случайного равновероятного выбора обратимого $p(x)$-циркулянта, $p(x) \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$. В силу изоморфизма алгебр $GCR_{p(x)}$ и $B_{p(x)}$ она полиномиально сводится к задаче случайного равновероятного выбора элемента из $B^*_{p(x)}$. Так как $p(x)$-циркулянт обратим тогда и только тогда, когда определяющий его многочлен взаимно прост с $p(x)$, то в случае приводимого $p(x)$ простейшим алгоритмом является выбор случайного многочлена $f(x) \in \mathbb{F}_q[x]$ степени не выше $n-1$ и вычисление значения $d(x) = \text{НОД}(f(x), p(x))$ в $\mathbb{F}_q[x]$. Если $d(x) \in \mathbb{F}^*_q$, то $f(x) \in B^*_{p(x)}$, иначе нужно выбирать новый $f(x)$. Ясно, что описанный метод является вероятностным типа Лас-Вегас, вследствие чего время его работы, а также количество запрошенных случайных элементов поля $\mathbb{F}_q$ могут сильно изменяться от запуска к запуску. Построим алгоритм случайного равновероятного выбора элемента из $B^*_{p(x)}$, свободный от указанных особенностей.

Пусть для многочлена $p(x)$ выполняется разложение (2.1) и

$$\mathbf{v}_{p(x)} = (p_1(x), p_2(x), \ldots, p_t(x)),$$
$$SF_{p(x)} = p_1(x)p_2(x)\cdots p_t(x).$$

Отметим, что многочлен $SF_{p(x)}$ свободен от квадратов. Через $\mathcal{O}_q$ и $\mathcal{O}^*_q$ обозначим вероятностные машины Тьюринга, получающие на вход ленту $\mathbf{1}^k$ с k ($\in \mathbb{N} \cup \{0\}$) непустыми ячейками и возвращающие случайно и равновероятно выбранный многочлен степени не выше $k-1$ из множеств $\mathbb{F}_q[x]$ и $\mathbb{F}_q[x] \setminus \{0\}$ соответственно (при $k = 0$ машины всегда возвращают нулевой многочлен). Дополнительно будем считать, что $\mathcal{O}_q$ и $\mathcal{O}^*_q$ всегда завершают свою работу за полиномиальное время относительно k и q, а также используют минимально возможное количество случайных элементов. Для краткости машины $\mathcal{O}_q$ и $\mathcal{O}^*_q$ будем называть *оракулами*.

Алгоритм GenPoly (случайный выбор элемента из $B^*_{p(x)}$).

Вход: *многочлен* $p(x)$ ($\in \mathbb{F}_q[x] \setminus \mathbb{F}_q$), *число* t – *количество неприводимых делителей* $p(x)$, *вектор* $\mathbf{v}_{p(x)}$, *многочлен* $SF_{p(x)}$.

Выход: *случайный элемент* $B^*_{p(x)}$.

Шаги алгоритма:

1. *Для* i *от* 1 *до* t *с шагом* 1 *вычислить* $g_i(x) = \mathcal{O}^*_q(\mathbf{1}^{\deg p_i(x)})$.
2. *Положить* $\mathbf{w} = (g_1(x), g_2(x), \ldots, g_t(x))$.
3. *Вычислить* $g(x) = \text{ResPoly}(\mathbf{w}, \mathbf{v}_{p(x)}, SF_{p(x)})$.
4. *Вычислить* $g_{n+1}(x) = \mathcal{O}_q(\mathbf{1}^{\deg p(x) - \deg SF_{p(x)}})$.
5. *Вычислить* $f(x) = g(x) + g_{n+1}(x) \cdot SF_{p(x)}$.
6. *Вернуть* $f(x)$ *и выйти из алгоритма.*

Конец алгоритма.

Замечание 1. Функция ResPoly, используемая на шаге 3, предназначена для вычисления такого многочлена $g(x)$ наименьшей степени из $B_{SF_{p(x)}}$, что для всех $i \in [1, t]$ выполняется сравнение $g(x) \equiv g_i(x) \pmod{p_i(x)}$. Разумно считать, что функция ResPoly детерминирована и имеет полиномиальную оценку временной сложности относительно степени $SF_{p(x)}$, количества делителей t и мощности поля $\mathbb{F}_q$. В качестве ResPoly можно воспользоваться, например, китайской теоремой об остатках для многочленов и соответствующим алгоритмом, описанным в [11; с. 473].

Замечание 2. Заметим, что

$$\deg g(x) < \deg p(x), \qquad \deg g_{n+1}(x) < \deg p(x) - \deg SF_{p(x)},$$

поэтому все операции на шаге 5 достаточно производить в кольце $\mathbb{F}_q[x]$.

Замечание 3. Для уменьшения вычислительной сложности алгоритма на шаге 1 можно параллельно использовать t оракулов.

Лемма 4. *Алгоритм* GenPoly *всегда завершает свою работу за конечное число шагов и возвращает равновероятно выбранный элемент из множества* $B^*_{p(x)}$.

Доказательство. Так как оракулы $\mathcal{O}_q$, $\mathcal{O}^*_q$ и функция ResPoly по предположению имеют полиномиальные оценки временной сложности, очевидно, что алгоритм всегда завершает свою работу за конечное число шагов.

Легко видеть, что вектор $\mathbf{w}$ всегда содержит ненулевые элементы и в силу описания оракула $\mathcal{O}^*_q$ является равновероятно выбранным элементом группы $G = B^*_{p_1(x)} \oplus \cdots \oplus B^*_{p_t(x)}$. В соответствии с леммой 1 группа G изоморфна группе $B^*_{SF_{p(x)}}$, причем изоморфизм осуществляется китайской теоремой об остатках, поэтому многочлен $g(x)$ является равновероятно выбранным элементом группы $B^*_{SF_{p(x)}}$.

Рассмотрим эпиморфизм γ алгебр $B_{p(x)}$ и $B_{SF_{p(x)}}$, имеющий ядром нильрадикал алгебры $B_{p(x)}$. Ясно, что сужение γ на $B^*_{p(x)}$ является эпиморфизмом групп $B^*_{p(x)}$ и $B^*_{SF_{p(x)}}$. Полный прообраз произвольного элемента $g(x) \in B^*_{SF_{p(x)}}$ есть

$$\gamma^{-1}(g(x)) = \{g(x) + n(x) \mid n(x) \in \operatorname{rad}(B_{p(x)})\} \subseteq B_p(x)^*,$$

поэтому если равновероятно и случайно перебирать многочлены $n(x) \in \operatorname{rad}(B_{p(x)})$, то многочлены $g(x) + n(x)$ будут равновероятно и случайно пробегать $\gamma^{-1}(g(x))$. Но в соответствии с доказательством леммы 1

$$\operatorname{rad}(B_{p(x)}) = (SF_{p(x)}) = \big\{d(x) \cdot SF_{p(x)} \mid d(x) \in \mathbb{F}_q[x],\ \deg d(x) < \deg p(x) - \deg SF_{p(x)}\big\},$$

что в сочетании с равновероятностью выбора $g(x)$ из $B^*_{SF_{p(x)}}$ и сюръективностью γ завершает доказательство леммы.

Вычислим оценку временной сложности алгоритма GenPoly в худшем случае. Будем полагать, что базовые операции в поле $\mathbb{F}_q$ (сложение, умножение, вычитание, деление, присвоение и сравнение элементов) имеют временную сложность $O(1)$. Через $R(k)$ обозначим количество операций в поле $\mathbb{F}_q$, выполняемых оракулами $\mathcal{O}_q$, $\mathcal{O}^*_q$ при работе с лентой $\mathbf{1}^k$, а через $F(t, n_{SF})$ обозначим количество операций в поле $\mathbb{F}_q$, выполняемых функцией ResPoly при запуске с параметрами $\mathbf{w}$, $\mathbf{v}_{p(x)}$, $SF_{p(x)}$, где t – длина векторов $\mathbf{v}_{p(x)}$, $\mathbf{w}$, а $n_{SF} = \deg SF_{p(x)}$. Пусть $M(m_1, m_2)$ – количество операций в поле $\mathbb{F}_q$, необходимых для умножения двух многочленов из $\mathbb{F}_q[x]$ степеней m_1 и m_2 соответственно. Тогда количество операций, выполняемых алгоритмом GenPoly, есть

$$O\bigg(\sum_{i=1}^{t} R(\deg p_i(x)) + R(n - n_{SF}) + F(t, n_{SF}) + M(n_{SF}, n - n_{SF})\bigg).$$

Если $R(k) = O(k)$, в качестве функции ResPoly используется китайская теорема об остатках и алгоритм из [11; с. 473], для которого $F(t, n_{SF}) = O(n^2_{SF})$, а для

умножения многочленов – алгоритм Карацубы [12; гл. 4.3.3], имеющий сложность $M(m_1, m_2) = O(\max\{m_1, m_2\}^{\log_2 3})$, то результирующая оценка сложности алгоритма GenPoly грубо упрощается до $O(n^2)$. Отметим, что если в функции ResPoly и на шаге 5 использовать более быстрые алгоритмы умножения многочленов, то оценку сложности можно уменьшить до субквадратичной.

Предположим, что оракулы $\mathcal{O}_q$, $\mathcal{O}_q^*$ при работе с лентой $\mathbf{1}^k$ используют не более k случайных элементов поля $\mathbb{F}_q$. Тогда общее количество случайных элементов, используемых алгоритмом GenPoly, не превышает n.

В заключение пункта отметим, что альтернативным к предлагаемому подходу методом построения многочленов $f(x) \in B^*_{p(x)}$ является рассмотрение корней $f(x)$ в некотором расширении $\mathbb{F}_{q^s}$ поля $\mathbb{F}_q$ (см., например, [13], для случая $p(x) = x^n - 1$). Действительно, взаимная простота $f(x)$ и $p(x)$ исключает наличие общих корней в поле разложения $\mathbb{F}_{q^s}$ обоих многочленов, поэтому для построения $f(x)$ можно случайно и равновероятно выбирать множество будущих корней из $\mathbb{F}_{q^s}$, не пересекающееся с корнями $p(x)$, и затем решать задачу интерполяции. Однако указанный подход либо требует арифметических действий в $\mathbb{F}_{q^s}$, где $s = n!$, либо требует работы со списком всех неприводимых многочленов кольца $\mathbb{F}_q[x]$ степени не выше n, что, по-видимому, практически неэффективно при довольно больших значениях n.

4. Алгоритмы построения $p(x)$-циркулянтов с фиксированным значением определителя. По-прежнему зафиксируем $p(x) \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$, элемент d поля $\mathbb{F}_q$ и рассмотрим задачу случайного равновероятного выбора $p(x)$-циркулянта со значением определителя d. В соответствии со следствием из леммы 3 элемент d должен принадлежать множеству $(\mathbb{F}_q^*)^m \cup \{0\}$. Как и ранее, под выбором $p(x)$-циркулянта будем понимать построение его определяющего многочлена.

4.1. Для случайного равновероятного выбора необратимого $p(x)$-циркулянта ($d = 0$) заменим первый шаг алгоритма GenPoly на следующие три:

1.1. *Вычислить* $I = \mathcal{O}_S^*(\mathbf{1}^t)$.

1.2. *Для каждого* $i \in I$ *присвоить* $g_i(x) = 0$.

1.3. *Для каждого* $i \in [1, t] \setminus I$ *вычислить* $g_i(x) = \mathcal{O}_q^*(\mathbf{1}^{\deg p_i(x)})$.

Здесь $\mathcal{O}_S^*(\mathbf{1}^t)$ – вероятностная машина Тьюринга, получающая на вход ленту $\mathbf{1}^t$ с t ($\in \mathbb{N}$) непустыми ячейками и возвращающая случайно выбраное непустое подмножество множества $[1, t]$ в соответствии со следующим распределением вероятностей:

$$\forall\, I \in 2^{[1,t]}, \quad I \neq \varnothing \qquad P\{\mathcal{O}_S^*(\mathbf{1}^t) = I\} = \frac{k(I)}{N_0}, \quad k(I) = \prod_{i \in [1,t] \setminus I} (q^{\deg p_i(x)} - 1),$$

где N_0 – общее количество векторов вида $(g_1(x), \ldots, g_t(x))$, $g_i(x) \in B_{p_i(x)}$, обладающих хотя бы одной нулевой компонентой. Легко проверяется, что описанная модификация алгоритма GenPoly позволит решить рассматриваемую задачу за конечное число шагов с учетом предположений о конечности времени работы машины $\mathcal{O}_S^*$ и используемом количестве случайных элементов.

4.2. Зафиксируем $d \in (\mathbb{F}_q^*)^m$ и рассмотрим задачу случайного равновероятного выбора $p(x)$-циркулянта из множества

$$B_{p(x)}(d) = \{c(x) \in B_{p(x)} \mid \det M_p(x)(\mathbf{c}) = d\}.$$

В соответствии со следствием из леммы 3 $B_{p(x)}(d)$ непусто. По аналогии с предыдущим случаем модифицируем алгоритм GenPoly так, чтобы на шаге 1 вектор $(g_1(x),\dots,g_t(x))$ случайно и равновероятно выбирался из множества

$$G_{p(x)}(d)=\left\{(g_1(x),\dots,g_t(x))\in B^*_{p_1(x)}\times\dots\times B^*_{p_t(x)}\;\Big|\;\prod_{i=1}^{t}(N_{p_i(x)}(g_i(x)))^{s_i}=d\right\}.$$

Легко видеть, что в таком случае алгоритм GenPoly будет случайно и равновероятно выбирать элементы $B_{p(x)}(d)$.

Модификацию шага 1 произведем следующим образом. Пусть $I=\{i_1,i_2,\dots,i_k\}\subseteq[1,t]$ – такое множество индексов наименьшей мощности, что

$$(m)=(s_{i_1})+(s_{i_2})+\dots+(s_{i_k})\qquad(\subseteq\mathbb{Z}_{q-1}).$$

Отметим, что если существует такой индекс $i\in[1,t]$, что $s_i=1$, то множество I всегда состоит из одного элемента. Без потери общности будем считать, что $I=[1,k]$. В силу леммы 3 имеет место равенство

$$\det M_{p(x)}(c(x))=\prod_{i=1}^{t}(N_{p_i(x)}(c_i(x)))^{s_i}=\prod_{j=1}^{k}(N_{p_j(x)}(c_j(x)))^{s_j}\cdot\prod_{i=k+1}^{t}(N_{p_i(x)}(c_i(x)))^{s_i},$$

где

$$\forall\, i\in[1,t]\qquad c_i(x)\equiv c(x)\pmod{p_i(x)}.$$

Для каждого $i\in[k+1,t]$ случайно равновероятно выберем элемент $g_i(x)$ из $B^*_{p_i(x)}$ и вычислим

$$d_1=\prod_{i=k+1}^{t}(N_{p_i(x)}(g_i(x)))^{s_i}\in(\mathbb{F}_q^*)^m.$$

Положим $d_2=d\cdot d_1^{-1}$ $(\in(\mathbb{F}_q^*)^m)$, $p^{(k)}(x)=p_1^{s_1}(x)\cdots p_k^{s_k}(x)$. В силу выбора I множество $G_{p^{(k)}(x)}(d_2)$ непусто, поэтому случайно равновероятно из него выберем элемент $(g_1(x),\dots,g_k(x))$ и составим вектор $\mathbf{w}=(g_1(x),\dots,g_k(x),g_{k+1}(x),\dots,g_t(x))$. Ясно, что $\mathbf{w}$ – случайно и равновероятно выбранный элемент $G_{p(x)}(d)$.

Описанную модификацию шага 1 формализуем следующим образом:

1.1. *Для i от $k+1$ до t с шагом 1 вычислить* $g_i(x)=\mathcal{O}_q^*(\mathbf{1}^{\deg p_i(x)})$.

1.2. *Вычислить* $d_1=\prod_{i=k+1}^{t}(N_{p_i(x)}(g_i(x)))^{s_i}$.

1.3. *Вычислить* $d_2=d\cdot d_1^{-1}$.

1.4. *Вычислить* $(g_1(x),\dots,g_k(x))=\mathcal{O}_{p(x)}(k,d_2)$, *где* $\mathcal{O}_{p(x)}(k,d_2)$ *– вероятностная машина Тьюринга, получающая на вход ленту с двумя заполненными ячейками, содержащими значения* k $(\in[1,t])$, d_2 $(\in(\mathbb{F}_q^*)^m)$, *и возвращающая случайно и равновероятно выбранный элемент из* $G_{p^{(k)}(x)}(d_2)$. *Отметим, что при выполнении данной модификации параметр k должен быть включен во вход алгоритма.*

Приведем оценку сложности предлагаемой модификации в наихудшем случае. Через $D(k,n)$ обозначим количество операций в поле $\mathbb{F}_q$, выполняемых оракулом $\mathcal{O}_{p(x)}$ при заполнении входной ленты значениями k и d_2, а через $N(\deg p(x),s)$ обозначим количество операций в поле $\mathbb{F}_q$, выполняемых при вычислении значения

$(N_{p(x)}(g(x)))^s$. Тогда количество операций, выполняемых описанной модификацией GenPoly, есть

$$O\biggl(\sum_{i=k+1}^{t}(R(\deg p_i(x))+N(\deg p_i(x),s_i))+D(k,n)\biggr).$$

В заключение отметим, что сложность рассматриваемой модификации алгоритма GenPoly зависит от степеней многочленов $p_i(x)$, $i\in I$, поэтому при выборе множества I необходимо учитывать эту особенность.

4.3. Построим алгоритм, реализующий работу оракула $\mathcal{O}_{p(x)}$ из предыдущего пункта. В полях $\mathbb{F}_q$, $B_{p_1(x)},\dots,B_{p_k(x)}$ зафиксируем примитивные элементы α, $a_1(x)$, $\dots,a_k(x)$ соответственно. Для каждого $i\in[1,k]$ через γ_i обозначим такое наименьшее целое неотрицательное число, что $N_{p_i(x)}(a_i(x))=\alpha^{\gamma_i}$, а через ℓ – такое наименьшее неотрицательное целое число, что $d_2=\alpha^{\ell}$.

Лемма 5. *Вектор*

$$(g_1(x),g_2(x),\dots,g_k(x))\in B^*_{p_1(x)}\times B^*_{p_2(x)}\times\dots\times B^*_{p_k(x)}$$

принадлежит множеству $G_{p^{(k)}(x)}(d_2)$ *тогда и только тогда, когда выполняется сравнение*

$$(s_1\gamma_1)h_1+(s_2\gamma_2)h_2+\dots+(s_k\gamma_k)h_k\equiv\ell\pmod{q-1},\tag{4.1}$$

где для каждого $i\in[1,k]$ *имеем*

$$0\leqslant h_i<q^{\deg p_i(x)}-1,\qquad (a_i(x))^{h_i}=g_i(x).$$

Доказательство. Утверждение проверяется прямыми вычислениями с учетом мультипликативности функции нормы.

В силу леммы 5 для случайного равновероятного выбора элемента из $G_{p^{(k)}(x)}(d_2)$ достаточно случайно и равновероятно выбирать решения сравнения (4.1) относительно неизвестных величин $h_1,\dots,h_k$ и вычислять вектор $((a_1(x))^{h_1},\dots,(a_k(x))^{h_k})$. Отметим, что переменные h_i в (4.1) принимают значения из множеств $[0,q^{\deg p_i(x)}-2]$ соответственно. Формализуем рассматриваемый способ в виде алгоритма. Положим $q_0=(q-1)/m$ и зафиксируем его разложение по степеням различных простых чисел

$$q_0=q_1^{e_1}q_2^{e_2}\cdots q_r^{e_r}.$$

Для каждого $i\in[1,k]$ определим

$$\ell_i=s_i\gamma_i\pmod{q-1},\qquad u_i=\frac{\ell_i}{m},$$

а для каждого $j\in[1,r]$ зафиксируем такое число $c_j\in[1,k]$, что НОД$(u_{c_j},q_j)=1$. Отметим, что существование c_j, $j\in[1,r]$, следует из того, что НОД$(u_1,\dots,u_k,q_0)=1$. Пусть $(x_1,\dots,x_k)\in\mathbb{Z}^k_{q-1}$ – некоторое решение сравнения

$$(s_1\gamma_1)x_1+(s_2\gamma_2)x_2+\dots+(s_k\gamma_k)x_k\equiv m\pmod{q-1}.$$

Через $\mathcal{O}_\infty$ обозначим вероятностную машину Тьюринга, которая получает на вход ленту $\mathbf{1}^l$ с l ($\in \mathbb{N} \cup \{0\}$) непустыми ячейками и возвращает случайно и равновероятно выбранное неотрицательное целое число из множества $[0, l-1]$. Дополнительно будем полагать, что $\mathcal{O}_\infty$ всегда завершает свою работу за полиномиальное время относительно $\log l$ и использует при этом минимально возможное количество случайных элементов (отметим, что всегда можно построить оракул $\mathcal{O}_\infty$, использующий $\log l + O(1)$ случайных бит).

Алгоритм RandChoice работы оракула $\mathcal{O}_{p(x)}$.
Вход: $k(\leqslant n) \in \mathbb{N}$, $d_2 \in \mathbb{F}_q^*$.
Выход: *элемент из* $G_{p^{(k)}(x)}(d_2)$ *или символ* $\perp$.
Шаги алгоритма.

1. *Вычислить такое наименьшее неотрицательное целое число* ℓ, *что* $d_2 = \alpha^\ell$.
2. *Вычислить* $\rho = \ell/m$. *Если* ℓ *не делится нацело на* m, *то вернуть символ* $\perp$ *и выйти из алгоритма*.
3. *Для* i *от* 1 *до* k *с шагом* 1 *вычислить* $\rho_i = x_i \cdot \rho \pmod{q-1}$.
4. *Для* j *от* 1 *до* r *с шагом* 1 *выполнить следующее*.
   4.1. *Для всех* $i \in \Lambda_j = [1,k] \setminus \{c_j\}$ *вычислить* $b_{ji} = \mathcal{O}_\infty(\mathbf{1}^{q_j^{e_j}})$.
   4.2. *Вычислить* $b_{jc_j} = -u_{c_j}^{-1} \sum_{i \in \Lambda_j} u_i b_{ji} \pmod{q_j^{e_j}}$.
5. *Для* i *от* 1 *до* k *с шагом* 1 *выполнить следующее*.
   5.1. *Вычислить* $b_i = \mathrm{ResNumb}((b_{1i}, \ldots, b_{ri}), (q_1^{e_1}, \ldots, q_r^{e_r}), q_0)$.
   5.2. *Вычислить* $\tau_i = \mathcal{O}_\infty(\mathbf{1}^m)$.
   5.3. *Вычислить* $z = (q^{\deg p_i(x)} - 1)/(q-1)$.
   5.4. *Вычислить* $\lambda_i = \mathcal{O}_\infty(\mathbf{1}^z)$.
   5.5. *Вычислить* $h_i = \rho_i + (b_i + \tau_i \cdot q_0 + \lambda_i \cdot (q-1)) \pmod{q^{\deg p_i(x)} - 1}$.
   5.6. *Вычислить* $g_i(x) = a_i^{h_i}(x)$.
6. *Вернуть вектор* $(g_1(x), g_2(x), \ldots, g_k(x))$ *и выйти из алгоритма*.

Конец алгоритма.

Замечание 4. Функция ResNumb, используемая на шаге 5, предназначена для вычисления такого элемента b_i из $\mathbb{Z}_{q_0}$, что для всех $j \in [1,r]$ выполняется сравнение $b_i \equiv b_{ji} \pmod{q_j^{e_j}}$. Будем считать, что ResNumb детерминирована и имеет полиномиальную оценку временной сложности относительно $\log q_0$ и количества делителей r. В качестве ResNumb можно воспользоваться, например, китайской теоремой об остатках для целых чисел и соответствующим алгоритмом, описанным в [11].

Лемма 6. *Алгоритм* RandChoice *всегда завершает свою работу за конечное число шагов и, если множество* $G_{p^{(k)}(x)}(d_2)$ *пусто, то возвращает символ* $\perp$, *иначе возвращает случайно и равновероятно выбранный элемент из* $G_{p^{(k)}(x)}(d_2)$.

Доказательство. Так как оракул $\mathcal{O}_\infty$ и функция ResNumb по предположению имеют полиномиальные оценки временной сложности, очевидно, что алгоритм всегда завершает свою работу за конечное число шагов.

Докажем корректность алгоритма. Для начала отметим, что разрешимость сравнения (4.1) однозначно определяется выполнимостью условия делимости ℓ на m, так как

$$\text{НОД}(s_1\gamma_1, s_2\gamma_2, \ldots, s_k\gamma_k, q-1) = \text{НОД}(s_1, s_2, \ldots, s_k, q-1) = m \tag{4.2}$$

(НОД$(\gamma_i, q-1) = 1$ для каждого $i \in [1,k]$). Пусть m делит ℓ. Легко проверяется, что вектор $(\rho_1, \rho_2, \ldots, \rho_k)$, компоненты которого вычисляются на шаге 3 алгоритма, является решением (4.1). Фиксация $(\rho_1, \rho_2, \ldots, \rho_k)$ устанавливает взаимно однозначное соответствие между всеми решениями сравнения (4.1) и всеми решениями однородного сравнения

$$(s_1\gamma_1)y_1 + (s_2\gamma_2)y_2 + \cdots + (s_k\gamma_k)y_k \equiv 0 \pmod{q-1} \tag{4.3}$$

вида $(y_1, y_2, \ldots, y_k)$, $0 \leqslant y_i < q^{\deg p_i(x)} - 1$, определяемое формулами

$$\forall\, i \in [1,k] \qquad h_i \equiv \rho_i + y_i \pmod{q^{\deg p_i(x)} - 1}.$$

В свою очередь множество решений сравнения (4.3) вида $(y_1, y_2, \ldots, y_k)$, $0 \leqslant y_i < q^{\deg p_i(x)} - 1$, может быть очевидным образом получено из множества решений вида $(\widehat{y}_1, \widehat{y}_2, \ldots, \widehat{y}_k)$, $0 \leqslant \widehat{y}_i < q-1$, того же сравнения по формулам

$$\forall\, i \in [1,k] \qquad y_i = \widehat{y}_i + \lambda_i(q-1),$$

где λ_i – произвольное число из множества $[0, (q^{\deg p_i(x)} - 1)/(q-1) - 1]$. В силу (4.2) решения $(\widehat{y}_1, \widehat{y}_2, \ldots, \widehat{y}_k)$ вычисляются из решений $(b_1, b_2, \ldots, b_k)$, $0 \leqslant b_i < q_0$, сравнения

$$\frac{s_1\gamma_1}{m}\, y_1 + \frac{s_2\gamma_2}{m}\, y_2 + \cdots + \frac{s_k\gamma_k}{m}\, y_k \equiv 0 \pmod{q_0} \tag{4.4}$$

по формулам

$$\forall\, i \in [1,k] \qquad \widehat{y}_i = b_i + \tau_i q_0,$$

где τ_i – произвольное число из множества $[0, q_0 - 1]$. Наконец, каждое решение (4.4) с помощью китайской теоремы об остатках может быть получено из множества решений вида $\{\{b_{ji}\}_{i\in[1,k]}\}_{j\in[1,r]}$, $0 \leqslant b_{ji} < q_j^{e_j}$, совокупности сравнений

$$\forall\, j \in [1,r] \qquad \frac{s_1\gamma_1}{m}\, b_{j1} + \frac{s_2\gamma_2}{m}\, b_{j2} + \cdots + \frac{s_k\gamma_k}{m}\, b_{jk} \equiv 0 \pmod{q_j^{e_j}}. \tag{4.5}$$

Алгоритм RandChoice на шаге 4 осуществляет случайный выбор решения совокупности (4.5), на шаге 5 вычисляет соответствующее решение сравнения (4.4), выполняет случайный подъем к решению вида $(y_1, y_2, \ldots, y_k)$, $0 \leqslant y_i < q^{\deg p_i(x)} - 1$, однородного сравнения (4.3), и получает в итоге искомое решение вида $(h_1, h_2, \ldots, h_k)$, $0 \leqslant h_i < q^{\deg p_i(x)} - 1$, сравнения (4.1), причем в силу предположения о работе оракула $\mathcal{O}_\infty$ любое из вычисляемых на шаге 5.5 решений равновозможно. Корректность алгоритма вытекает теперь из утверждения леммы 5.

Приведем оценку временной сложности алгоритма RandChoice в худшем случае. Для этого расширим модель вычислений и будем дополнительно полагать, что базовые операции в кольце вычетов $\mathbb{Z}_{q-1}$ (сложение, умножение, вычитание, деление, присвоение и сравнение элементов) имеют временную сложность $O(1)$. Можно считать, что временная сложность шага 1 есть $O(\sqrt{q}\,)$ (например, в случае использования алгоритма согласования Гельфонда). Через $R_\infty(\log l)$ обозначим функцию сложности оракула $\mathcal{O}_\infty$ при работе с лентой $\mathbf{1}^l$, а через $CD(q, \deg f(x)))$ – сложность возведения в степень h, $0 \leqslant h < q^{\deg f(x)} - 1$, примитивного элемента $a(x)$ в поле $B_{f(x)}$.

Нетрудно видеть, что вычислительная сложность алгоритма RandChoice при этом в наихудшем случае есть

$$O\biggl(r\cdot k + R_\infty(L\log q) + \sum_{i=1}^{k} CD(q, \deg p_i(x))\biggr), \qquad L = \sum_{i=1}^{k} \deg p_i(x),$$

а общее число используемых случайных бит не превосходит $L\log q + O(1)$.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[1] В. В. Воеводин, Е. Е. Тыртышников, *Вычислительные процессы с теплицевыми матрицами*, Наука, М., 1987.

[2] Zhao-Lin Jiang, Zong-Ben Xu, "Efficient algorithm for finding the inverse and the group inverse of FLS r-circulant matrix", *J. Appl. Math. Comput.*, **18**:1-2 (2005), 45–57.

[3] Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн, *Теория кодов, исправляющих ошибки*, Связь, М., 1979.

[4] D. Chillag, "Regular representations of semisimple algebras, separable field extensions, group characters,generalized circulants, and generalized cyclic codes", *Linear Algebra Appl.*, **218** (1995), 147–183.

[5] A. Mahalanobis, "The discrete logarithm problem in the group of non-singular circulant matrices", *Groups Complex. Cryptol.*, **2**:1 (2010), 83–89.

[6] R. J. McEliece, *A Public-Key Cryptosystem Based on Algebraic Coding Theory*, Deep Space Network Progress Report, DSN PR 42-44, 1978, 114–116.

[7] A. D. Wyner, "The Wire-Tap Channel", *Bell System Tech. J.*, **54**:8 (1975), 1355–1387.

[8] L. H. Ozarow, A. D. Wyner, "Wire-tap channel. II", *Advances in Cryptology*, Lecture Notes in Comput. Sci., **209**, Springer, Berlin, 1985, 33–50.

[9] Р. Лидл, Г. Нидеррайтер, *Конечные поля*, Т. 1, Мир, М., 1988.

[10] Ф. Р. Гантмахер, *Теория матриц*, Наука, М., 1988.

[11] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge Univ. Press, Cambridge, 2009.

[12] Д. Кнут, *Искусство программирования*. Т. 2. *Получисленные алгоритмы*, Мир, М., 2000.

[13] В. В. Гриценко, Ю. В. Косолапов, "Построение всех обратимых циркулянтов над полями Галуа", *Изв. Вузов. Сев.-кавказск. регион. Сер. Естеств. науки*, **2** (2012), 8–12.

В. В. Гриценко
Южный федеральный университет,
г. Ростов-на-Дону
E-mail: gritsenko.vld@gmail.com

Поступило
04.08.2013

А. Э. Маевский
Южный федеральный университет,
г. Ростов-на-Дону
E-mail: tim_org@mail.ru