Записки научных
семинаров ПОМИ
Том 490, 2020 г.

В. Г. Журавлев

$\mathcal{L}$-АЛГОРИТМ АППРОКСИМАЦИИ ДИОФАНТОВЫХ СИСТЕМ ЛИНЕЙНЫХ ФОРМ

Введение

0.1. Основной результат. Рассмотрим произвольное алгебраическое поле $\mathbb{Q}(\alpha)=\mathbb{Q}(\alpha_1,\ldots,\alpha_d)$ – алгебраическое расширение степени $d+1\geqslant 2$ поля рациональных чисел $\mathbb{Q}$ добавлением к нему чисел $\alpha_1,\ldots,\alpha_d$; и пусть $1\leqslant k\leqslant d$ обозначает количество некоторых произвольных фиксированных сопряжений поля $\mathbb{Q}(\alpha)$ с условием, что комплексные сопряжения считаются парами. В предложении 2.1 доказано существование унимодулярной матрицы $\mathrm{P}_\alpha\in\mathrm{GL}_{d+1}(\mathbb{Z})$, для которой столбец $\widehat{\alpha}=\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_d\\ 1\end{pmatrix}$ является собственным

$$\mathrm{P}_\alpha\widehat{\alpha}=\lambda\cdot\widehat{\alpha}. \tag{0.1}$$

Здесь λ – локализованная единица поля $\mathbb{Q}(\alpha)$: ровно k выделенных ее сопряженных обладает свойством $|\lambda^{(j)}|>1$.

Выделим в $\mathbb{R}^{d+1}$ подпространство $A_+\subset\mathbb{R}^{d+1}$, натянутое на векторы $\widehat{\alpha}^{(i)}$ для вещественных выделенных сопряжений и парные векторы $\widehat{\alpha}^{(j)}_+=\frac{1}{2}(\widehat{\alpha}^{(j)}+\overline{\widehat{\alpha}}^{(j)})$, $\widehat{\alpha}^{(j)}_-=\frac{1}{2i}(\widehat{\alpha}^{(j)}-\overline{\widehat{\alpha}}^{(j)})$ для комплексных сопряжений. Обозначим через $A_+^\perp\subset\mathbb{R}^{d+1}$ подпространство, ортогональное $A_+^\perp\ \perp A_+$ к A_+. Далее, выберем в пространстве $A_+^\perp$ произвольный базис

$$\alpha_1^\perp=(\alpha_{1,1}^\perp,\ldots,\alpha_{1,d+1}^\perp),\ldots,\alpha_{k^\perp}^\perp=(\alpha_{k^\perp,1}^\perp,\ldots,\alpha_{k^\perp,d+1}^\perp), \tag{0.2}$$

где $k^\perp=\dim_{\mathbb{Q}}A_+^\perp$ – размерность пространства $A_+^\perp$, определяемая из равенства $k+k^\perp=d+1$. Базису (0.2) поставим в соответствие систему

Ключевые слова: диофантовы приближения линейных форм, симплекс-модульный алгоритм, наилучшие приближения.

линейных форм

$$\begin{aligned} F_1(x) &= \alpha^{\perp}_{1,1}x_1 + \ldots + \alpha^{\perp}_{1,d+1}x_{d+1}, \\ &\ldots \\ F_{k^{\perp}}(x) &= \alpha^{\perp}_{k^{\perp},1}x_1 + \ldots + \alpha^{\perp}_{k^{\perp},d+1}x_{d+1} \end{aligned} \tag{0.3}$$

с вещественными коэффициентами. Из построения следует, что линейные формы (0.3) образуют базис в пространстве $F^{\perp}_{+}$ всех линейных форм $F_{\alpha^{\perp}}(x)$, где $\alpha^{\perp} \in A^{\perp}_{+}$. В теореме 4.1 доказано следующее утверждение.

Существует последовательность целочисленных точек $p_a = (p_{a,1}, \ldots, p_{a,d+1})$, *удовлетворяющих рекуррентному соотношению, определяемому характеристическим многочленом*

$$ch_{P_\alpha}(x) = \det(xE - \mathrm{P}_\alpha)$$

унимодулярной матрицы P_α *из* (0.1), *такая что выполняется система неравенств*

$$\begin{aligned} |F_1(p_a)| &\leqslant \frac{C}{|p_a|_s^{\theta}}, \\ &\ldots \\ |F_{k^{\perp}}(p_a)| &\leqslant \frac{C}{|p_a|_s^{\theta}} \end{aligned} \tag{0.4}$$

для всех $a = 0, 1, 2, \ldots$ *Здесь показатель* $\theta = \frac{k}{k^{\perp}} - \varrho$, *при этом отклонение* $\varrho > 0$ *можно сделать сколь угодно малым за счет подходящего выбора матрицы* P_α *в* (0.1); *константа* C *не зависит от номера итерации* a; *величина* $|p_a|_s = |p_{a,1}| + \ldots + |p_{a,d+1}|$ *имеет экспоненциальный рост при* $a \to +\infty$.

0.2. История вопроса. По одному из следствий теоремы Дирихле ([1], с. 30) существует бесконечно много целочисленных решений p_a системы неравенств (0.4) с показателем $\theta = \frac{k}{k^{\perp}}$. В настоящей работе мы предлагаем $\mathcal{L}$-алгоритм построения таких решений. Указанный алгоритм опирается на метод локализации единиц алгебраических числовых полей [2–4]. Ранее [3] первоначальный вариант $\mathcal{L}$-алгоритма – обратный симплекс-модульный алгоритм – был применен к системам неравенств (0.4) частного вида, когда $k^{\perp} = 1$. Среди многочисленных исследований по диофантовым приближениям линейных форм выделим работы [5,6], где для тернарных форм были построены наилучшие приближения.

§1. Локализация единиц алгебраических полей

1.1. Единицы алгебраических полей. Рассмотрим произвольное алгебраическое поле

$$\mathbb{F} = \mathbb{Q}(\theta) \subset \mathbb{C} \tag{1.1}$$

– алгебраическое расширение степени $d+1 = r+2c$ поля рациональных чисел $\mathbb{Q}$, где r и $2c$ обозначают число вещественных и комплексных сопряжений соответственно (подробности см., например, [7]). Выберем в $\mathbb{F}$ некоторую *полную систему единиц*

$$\varepsilon_1, \ldots, \varepsilon_t, \tag{1.2}$$

где $t = r + c - 1$. Отметим, что система единиц (1.2) не обязана порождать всю группу единиц поля $\mathbb{F}$. Требуется лишь, чтобы единицы из (1.2) были свободными образующими порождаемой ими *группы единиц* $\mathcal{E}$ и данная группа имела бы максимально возможный *ранг* t.

Зададим отображение

$$\varepsilon \quad \mapsto \quad x(\varepsilon) = (\ln|\varepsilon^{(1)}|, \ldots, \ln|\varepsilon^{(r)}|, 2\ln|\varepsilon^{(r+1)}|), \ldots, 2\ln|\varepsilon^{(r+c)}|) \tag{1.3}$$

множества единиц $\mathcal{E}$ в пространство $\mathbb{R}^{t+1}$, где $\varepsilon^{(1)}, \ldots, \varepsilon^{(r)}$ – вещественные сопряженные значения для ε и $\varepsilon^{(r+1)}, \ldots, \varepsilon^{(r+c)}$ – комплексные. Отображение (1.3) будет вложением $x : \mathcal{E} \hookrightarrow \mathbb{R}^{t+1}$ группы $\mathcal{E}$ в векторное пространство $\mathbb{R}^{t+1}$ с сохранением в них операций

$$x(\varepsilon \cdot \varepsilon') = x(\varepsilon) + x(\varepsilon'). \tag{1.4}$$

1.2. Локализация. Из определения отображения (1.3) следует, что образ $\mathcal{L} = x(\mathcal{E})$ группы единиц $\mathcal{E}$ содержится в гиперплоскости

$$P \quad = \{x \in \mathbb{R}^{t+1}; \quad \mathbf{n} \cdot x = 0\}, \tag{1.5}$$

где $\mathbf{n} \cdot x$ – скалярное произведение x с вектором $\mathbf{n} = (1, \ldots, 1)$ размерности $t+1$. Подмножество $\mathcal{L} \subset P$ предствляет собою *полную решетку* в пространстве (1.5) с $\mathbb{Z}$-*базисом* $x(\varepsilon_1), \ldots, x(\varepsilon_t)$. Данное множество также образует базис в P, но уже относительно $\mathbb{R}$.

Пусть

$$k = k_r + 2k_c, \tag{1.6}$$

где $0 \leqslant k_r \leqslant r$ и $0 \leqslant k_c \leqslant c$ – целые числа, удовлетворяет неравенствам

$$1 \leqslant k \leqslant d. \tag{1.7}$$

Определим вектор
$$\mu_k = \mu_{k_r,k_c} = (\underbrace{\ldots,\mu,\ldots,-1,\ldots}_{r},\underbrace{\ldots,2\mu,\ldots,-2,\ldots}_{c}) \tag{1.8}$$
с координатами μ или -1 на первых r местах и соответственно координатами 2μ или -2 на остальных c местах. При этом количество координат μ равно k_r, а 2μ равно k_c. Будем предполагать, что вектор (1.8) принадлежит
$$\mu_k \in P \tag{1.9}$$
– гиперплоскости (1.5). Тогда μ в (1.8) должно быть равным
$$\mu = \frac{d-k+1}{k} \tag{1.10}$$
и при этом в силу (1.7) удовлетворять неравенствам
$$\frac{1}{d} \leqslant \mu \leqslant d. \tag{1.11}$$

Из включения (1.9) следует, что вектор μ_k разложим
$$\mu_k = \beta_1 x(\varepsilon_1) + \ldots + \beta_t x(\varepsilon_t) \tag{1.12}$$
по базису решетки $\mathcal{L}$ с некоторыми вещественными коэффициентами $\beta_1,\ldots,\beta_t$. Теперь воспользуемся одним результатом из [3].

Следствие 1.1. *Пусть $\beta = (\beta_1,\ldots,\beta_t)$ – любой вещественный вектор и $\eta > 0$ – произвольное наперед заданное сколь угодно малое число. Тогда найдется такое натуральное число q, что будет выполняться неравенство*
$$||q\beta||_s = ||q\beta_1|| + \ldots + ||q\beta_t|| \leqslant \eta, \tag{1.13}$$
где $||x||$ обозначает расстояние от x до ближайшего целого числа.

Замечание 1.1. В [8] был построен симплекс-ядерный алгоритм разложения в многомерные цепные дроби. Указанный алгоритм позволяет находить натуральные числа q с условием (1.13).

По следствию 1.1 для любого произвольного наперед заданного сколь угодно малого числа $\eta > 0$ найдутся такие целые числа $q \geqslant 1$ и $p_1,\ldots,p_t$, что будет выполняться неравенство
$$|q\beta - p|_s = |q\beta_1 - p_1| + \ldots + |q\beta_t - p_t| \leqslant \eta \tag{1.14}$$
в метрике $|x|_s = |x_1| + \ldots + |x_t|$ для $x = (x_1,\ldots,x_t)$ из $\mathbb{R}^t$.

Выберем единицу
$$\zeta = \varepsilon_1^{p_1} \cdots \varepsilon_t^{p_t}. \tag{1.15}$$

Для нее, согласно свойству (1.4), имеем

$$x(\zeta) = p_1 x(\varepsilon_1) + \ldots + p_t x(\varepsilon_t). \tag{1.16}$$

Из (1.8) и (1.12) следует равенство

$$q\mu_k = q\beta_1 x(\varepsilon_1) + \ldots + q\beta_t x(\varepsilon_t),$$

из которого и (1.16) находим разность

$$q\mu_k - x(\zeta) = (q\beta_1 - p_1)x(\varepsilon_1) + \ldots + (q\beta_t - p_t)x(\varepsilon_t).$$

Запишем векторы

$$x(\varepsilon_i) = (x_1(\varepsilon_i), \ldots, x_{t+1}(\varepsilon_i)) \tag{1.17}$$

в координатах пространства $\mathbb{R}^{t+1}$. Тогда разность векторов $q\mu_k - x(\zeta)$ в силу (1.14) оценивается как

$$|q\mu_k - x(\zeta)|_s \leqslant \eta', \tag{1.18}$$

где справа обозначили $\eta' = \eta\,(t+1)\,\max_\varepsilon$ и

$$\max_\varepsilon = \max_{\substack{1\leqslant i\leqslant t\\ 1\leqslant j\leqslant t+1}} |x_j(\varepsilon_i)|. \tag{1.19}$$

Если ввести обозначение

$$\varrho = (\varrho_1, \ldots, \varrho_{t+1}) = x(\zeta) - q\mu_k,$$

то для вектора $x(\zeta)$ получим представление

$$x(\zeta) = q\mu_k + \varrho, \tag{1.20}$$

при этом координаты вектора ϱ по (1.18) удовлетворяют неравенствам

$$|\varrho_1| \leqslant \eta', \quad \ldots, \quad |\varrho_t| \leqslant \eta'. \tag{1.21}$$

По определению (1.3) записываем

$$x(\zeta) = (\underbrace{\ln|\zeta^{(1)}|, \ln|\zeta^{(2)}|, \ldots, \ln|\zeta^{(r)}|}_{r}, \underbrace{2\ln|\zeta^{(r+1)}|), \ldots, 2\ln|\zeta^{(r+c)}|}_{c}), \tag{1.22}$$

а по (1.8) имеем

$$q\mu_k = (\underbrace{\ldots, q\mu, \ldots, -q, \ldots}_{r}, \underbrace{\ldots, 2q\mu, \ldots, -2q, \ldots}_{c}). \tag{1.23}$$

Для сопряженных значений $\zeta^{(i)}$ единицы ζ в (1.22) введем нумерацию

$$\underbrace{\ldots, \zeta^{(i_+)}, \ldots, \zeta^{(i_-)}, \ldots}_{r}, \quad \underbrace{\ldots, \zeta^{(j_+)}, \ldots, \zeta^{(j_-)}, \ldots}_{c} \tag{1.24}$$

в соответствии с координатами вектора (1.23). В этой нумерации сравнивая координаты векторов (1.22), (1.23) и используя разложение (1.20), приходим к следующим формулам

$$\begin{aligned} \ln|\zeta^{(i_+)}| = q\mu + \varrho_{i_+}, \quad \ln|\zeta^{(i_-)}| = -q + \varrho_{i_-}, \\ \ln|\zeta^{(j_+)}| = q\mu + \varrho_{j_+}, \quad \ln|\zeta^{(j_-)}| = -q + \varrho_{j_-}. \end{aligned} \tag{1.25}$$

Сделаем замену

$$\ln\zeta_+ = q\mu \tag{1.26}$$

в формулах (1.25). Имеем

$$\begin{aligned} \ln|\zeta^{(i_+)}| = \ln\zeta_+ + \varrho_{i_+}, \quad \ln|\zeta^{(i_-)}| = \ln\zeta_+^{-1/\mu} + \varrho_{i_-}, \\ \ln|\zeta^{(j_+)}| = \ln\zeta_+ + \varrho_{j_+}, \quad \ln|\zeta^{(j_-)}| = \ln\zeta_+^{-1/\mu} + \varrho_{j_-} \end{aligned} \tag{1.27}$$

или без логарифмов –

$$\begin{aligned} |\zeta^{(i_+)}| = \zeta_+^{1+\theta_{i_+}}, \quad |\zeta^{(i_-)}| = \zeta_+^{-1/\mu+\theta_{i_-}}, \\ |\zeta^{(j_+)}| = \zeta_+^{1+\theta_{j_+}}, \quad |\zeta^{(j_-)}| = \zeta_+^{-1/\mu+\theta_{j_-}}, \end{aligned} \tag{1.28}$$

где

$$\theta_i = \varrho_i/\ln\zeta_+, \tag{1.29}$$

при этом ϱ_i удовлетворяют неравенствам (1.21).

Предложение 1.1. *Пусть* $\varepsilon = \{\varepsilon_1, \ldots, \varepsilon_t\}$ *– некоторая полная система единиц* (1.2) *алгебраического поля* $\mathbb{F}$ *из* (1.1) *степени* $d+1$, ζ *– единица* (1.15)*, зависящая от* $\eta > 0$*, и* $\zeta^{(i)}$ *– ее сопряженные; и пусть параметр* k *из* (1.6) *удовлетворяет неравенствам* $1 \leqslant k \leqslant d$. *Тогда существует такая константа* $\eta_\varepsilon > 0$*, зависящая от выбора системы единиц* ε*, что для*

$$0 < \eta < \eta_\varepsilon, \tag{1.30}$$

выполняются следующие свойства.

1) *Модули сопряженных* $\zeta^{(i)}$ *вычисляются по формулам* (1.28) *с показателями*

$$|\theta_i| \leqslant c_\varepsilon \eta, \tag{1.31}$$

где константа $c_\varepsilon > 0$ *не зависит от выбора параметра* η *из* (1.30).

2) *Сопряженные* $\zeta^{(i)}$ *распределяются по группам*

$$\begin{aligned} |\zeta^{(i_+)}| > 1, \quad |\zeta^{(i_-)}| < 1, \\ |\zeta^{(j_+)}| > 1, \quad |\zeta^{(j_-)}| < 1. \end{aligned} \tag{1.32}$$

Доказательство. В силу уже выведенных формул (1.28) для доказательства первого утверждения нужно проверить выполнимость неравенств (1.31). Принимая во внимание (1.29) и (1.21), записываем

$$|\theta_i| \leqslant \frac{\eta'}{\ln\zeta_+} \leqslant c_\varepsilon \eta, \tag{1.33}$$

где константа

$$c_\varepsilon = \frac{(t+1)\max_\varepsilon}{\ln\zeta_+}$$

не зависит от η.

Для доказательства второго утверждения заметим, что из (1.11), (1.26) следует $\zeta_+ > 1$, поэтому в силу формул (1.28) неравенства (1.26) будут выполняться при достаточно малом $\eta_\varepsilon > 0$. □

1.3. Локализованные единицы. Числа

$$\zeta = \zeta_{k,\eta} \tag{1.34}$$

будем называть *локализованными единицами* с параметрами k из (1.6), (1.7) и η из интервала (1.30). Их основное свойство состоит в том, что их сопряженные $\zeta^{(i)}$ распределяются по группам (1.32) и модули $|\zeta^{(i)}|$ содержатся соответственно в двух окрестностях

$$\begin{gathered}
\zeta_+ - \delta_\eta \leqslant |\zeta^{(i_+)}| \leqslant \zeta_+ + \delta_\eta, \qquad \zeta_+ - \delta_\eta \leqslant |\zeta^{(j_+)}| \leqslant \zeta_+ + \delta_\eta,\\
\zeta_+^{-1/\mu} - \delta_\eta \leqslant |\zeta^{(i_-)}| \leqslant \zeta_+^{-1/\mu} + \delta_\eta, \quad \zeta_+^{-1/\mu} - \delta_\eta \leqslant |\zeta^{(j_-)}| \leqslant \zeta_+^{-1/\mu} + \delta_\eta,
\end{gathered} \tag{1.35}$$

где $\zeta_+ > 1$ не зависит от выбора параметра η из (1.30) и величена отклонения $\delta_\eta \downarrow 0$, если $\eta \to 0$. Свойство локализации (1.35) единиц ζ вытекает из формул (1.28) и неравенств (1.30), (1.31).

Обозначим через

$$\mathcal{E}_{k,\eta} \subset \mathcal{E} \tag{1.36}$$

подмножество всех единиц ζ из группы $\mathcal{E}$, удовлетворяющих условию (1.32). Из свойства (1.4) следует замкнутость множества $\mathcal{E}_{k,\eta}$ относительно умножения $\zeta \cdot \zeta' \in \mathcal{E}_{k,\eta}$ для любых $\zeta, \zeta' \in \mathcal{E}_{k,\eta}$. Поэтому множество $\mathcal{E}_{k,\eta}$ образует *полугруппу* без единицы, поскольку 1 не обладает свойством (1.32).

Пусть элемент α принадлежит алгебраическому полю $\mathbb{F}$ из (1.1) и k – параметр (1.6), (1.7). Предположим, что α имеет степень

$$\deg(\alpha) < d + 1. \tag{1.37}$$

Здесь *степень* $\deg(\alpha)$ числа α определяется равенством

$$\deg(\alpha) = \deg \mathbb{Q}(\alpha), \tag{1.38}$$

где справа указана степень $\deg \mathbb{Q}(\alpha) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ расширения $\mathbb{Q}(\alpha)$ над полем $\mathbb{Q}$. Тогда найдутся такие $l \neq m$, что имеет место равенство

$$\alpha^{(l)} = \alpha^{(m)}. \tag{1.39}$$

Кроме того предположим, что сопряженные $\alpha^{(i)}$ для α распределяются по группам

$$\begin{array}{ll} |\alpha^{(i_+)}| > 1, & |\alpha^{(i_-)}| < 1, \\ |\alpha^{(j_+)}| > 1, & |\alpha^{(j_-)}| < 1 \end{array} \tag{1.40}$$

аналогично (1.32). Скажем, что элемент α *согласован* с параметром k, если свойства (1.39) и (1.40) не противоречат друг другу для всех $l \neq m$.

Предложение 1.2. *Если выполнены условия предложения* 1.1 *и ранг* $t \geqslant 1$*, то*

1) *полугруппа* $\mathcal{E}_{k,\eta} \neq \varnothing$*;*

2) *любая единица* $\zeta \in \mathcal{E}_{k,\eta}$*, несогласованная с параметром* k*, имеет степень*

$$\deg(\zeta) = d + 1. \tag{1.41}$$

Доказательство. Первое утверждение вытекает из предложения 1.1. Второе докажем от противного: предположим степень

$$\deg(\zeta) < d + 1.$$

Тогда из этого неравенства и несогласованости ζ с параметром k следует, что найдутся $l \neq m$, для которых будут выполняться противоречащие друг другу свойства (1.39) и (1.40) для $\alpha = \zeta$. □

§2. Модульные $\mathcal{L}$-матрицы

2.1. Модули. Обозначим через

$$\mathcal{L} = \mathcal{L}_{k,\eta} \subset \mathcal{E}_{k,\eta} \tag{2.1}$$

подмножество всех единиц ζ из полугруппы (1.36), несогласованных с параметром k, и назовем их *$\mathcal{L}$-единицами*. Если $\zeta \in \mathcal{L}$, то по предложению 1.2 ее степени $1, \zeta, \dots, \zeta^d$ линейно независимы над $\mathbb{Q}$. Поэтому алгебраическое поле $\mathbb{Q}(\zeta)$ совпадает

$$\mathbb{Q}(\zeta) = \mathbb{F} \tag{2.2}$$

с полем (1.1) и *модуль*

$$\mathcal{M}_\zeta = \mathbb{Z}[1, \zeta, \dots, \zeta^d] \tag{2.3}$$

над кольцом $\mathbb{Z}$ будет *полным*, т.е. числа $1, \zeta, \ldots, \zeta^d$ образуют базис поля $\mathbb{F}$ над $\mathbb{Q}$.

Рассмотрим линейное отображение

$$\mathcal{M}_\zeta \xrightarrow{\zeta} \mathcal{M}_\zeta : \quad x \mapsto \zeta \cdot x. \tag{2.4}$$

Из определения (2.3) вытекает, что отображение (2.4) задает автоморфизм модуля $\mathcal{M}_\zeta$. Поскольку $1, \zeta, \ldots, \zeta^d$ – базис модуля $\mathcal{M}_\zeta$, то найдется квадратная унимодулярная матрица U_ζ размера $d+1$, удовлетворяющая условию

$$U_\zeta \widehat{\zeta} = \zeta \cdot \widehat{\zeta}, \tag{2.5}$$

где слева записано произведение матрицы U_ζ и столбца

$$\widehat{\zeta} = \begin{pmatrix} \zeta^d \\ \vdots \\ \zeta \\ 1 \end{pmatrix} \tag{2.6}$$

высоты $d+1$. Матрица U_ζ называется *матрицей предствления* элемента ζ в базисе $1, \zeta, \ldots, \zeta^d$.

2.2. Матрица перехода T. Пусть

$$\mathcal{M}_\alpha = \mathbb{Z}[1, \alpha_1, \ldots, \alpha_d] \tag{2.7}$$

– произвольный полный модуль над кольцом $\mathbb{Z}$ в поле $\mathbb{F}$. Точку $\alpha = (\alpha_1, \ldots, \alpha_d)$ и соответствующий набор чисел $\{\alpha_1, \ldots, \alpha_d\}$, обладающие свойством (2.7), будем называть *полными*. Для полной точки α характерно выполнение соотношения

$$\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha) \tag{2.8}$$

между $\mathbb{Q}[\alpha]$ – модулем (2.7) и $\mathbb{Q}(\alpha)$ – расширением поля рациональных чисел $\mathbb{Q}$ добавлением к нему чисел $\alpha_1, \ldots, \alpha_d$. Из (2.7) и (2.8), в частности, следует иррациональность точки $\alpha = (\alpha_1, \ldots, \alpha_d)$ и равенство $\mathbb{Q}(\alpha) = \mathbb{F}$, а значит, полная точка α имеет степень

$$\deg \alpha = d + 1. \tag{2.9}$$

Вектор или точку α назовем *иррациональными*, если выполняется условие:

$$\textit{числа} \ \ 1, \alpha_1, \ldots, \alpha_d \ \textit{линейно независимы над кольцом} \ \ \mathbb{Z}. \tag{2.10}$$

Далее, пусть T – *матрица перехода*

$$\widehat{\alpha} = T\widehat{\zeta} \tag{2.11}$$

от базиса полного модуля $\mathcal{M}_\zeta$ к базису модуля $\mathcal{M}_\alpha$. Здесь столбец $\widehat{\alpha}$ определяется по модулю $\mathcal{M}_\alpha$ добавлением единицы

$$\widehat{\alpha} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_d \\ 1 \end{pmatrix}. \tag{2.12}$$

Матрица перехода T имеет рациональные коэффициенты. Кроме того, поскольку модуль $\mathcal{M}_\alpha$ также полный, то матрица T обратима и, значит, $T \in \mathrm{GL}_{d+1}(\mathbb{Q})$.

2.3. Модульные матрицы. Воспользуемся (2.11) и подставим $\widehat{\zeta} = T^{-1}\widehat{\alpha}$ в равенство (2.5). Имеем

$$U_\zeta T^{-1}\widehat{\alpha} = \zeta \cdot T^{-1},$$

откуда для столбца $\widehat{\alpha}$ выводим равенство

$$M_\alpha \widehat{\alpha} = \zeta \cdot \widehat{\alpha} \tag{2.13}$$

с рациональной матрицей

$$M_\alpha = T U_\zeta T^{-1}, \tag{2.14}$$

сопряженной унимодулярной матрице U_ζ. Для модуля $\mathcal{M}_\alpha$ из (2.7) матрицу, обладающую свойством (2.13), назовем *модульной матрицей.*

2.4. Унимодулярные модульные матрицы. *Уровень*

$$l(T) = t \tag{2.15}$$

невырожденной рациональной матрицы T определяется как наименьшее натуральное число t с условием, что $T^* = t \cdot T^{-1}$ – целочисленная матрица.

Нам потребуется еще *показатель* $\nu_a(U_\zeta) = \nu$ унимодулярной матрицы U_ζ по модулю t – это такое наименьшее натуральное число ν, для которого выполняется сравнение

$$U_\zeta^\nu \equiv E \bmod t, \tag{2.16}$$

где $E = E_{d+1}$ – единичная матрица размера $d+1$. Указанное число ν существует и не превышает порядка конечной группы $\mathrm{GL}_{d+1}(\mathbb{Z}/t\mathbb{Z})$ матриц над кольцом вычетов $\mathbb{Z}/t\mathbb{Z}$ с определителем $\det \equiv \pm 1 \bmod t$.

Предложение 2.1. *Если $\mathcal{M}_\alpha$ – произвольный полный модуль* (2.7) *из поля $\mathbb{F}$, t – уровень* (2.15) *матрицы T и ν – показатель* (2.16) *унимодулярной матрицы U_ζ по модулю t, то* 1) *матрица*

$$\mathrm{P}_\alpha = M_\alpha^\nu \tag{2.17}$$

является унимодулярной; 2) *имеет место равенство*

$$\mathrm{P}_\alpha \widehat{\alpha} = \lambda \cdot \widehat{\alpha}, \tag{2.18}$$

где $\widehat{\alpha}$ – столбец (2.12) *и*

$$\lambda = \zeta^\nu \tag{2.19}$$

является $\mathcal{L}$-единицей из множества (2.1).

Доказательство. Равенства (2.17) и (2.18) были доказаны в [9] и нужно проверить, что λ – $\mathcal{L}$-единица. Действительно, из равенства (2.19) и свойства мультипликативности следует выполнимость неравенств (1.32) для λ, а из (1.15) выводим равенство $\deg(\lambda) = d+1$, из которого вытекает несогласованность λ с параметром k. □

Матрицу P_α из (2.17) назовем *унимодулярной модульной матрицей.* Если при этом ζ является $\mathcal{L}$-единицей, то P_α будем также называть *модульной $\mathcal{L}$-матрицей* или кратко – *$\mathcal{L}$-матрицей.*

§3. Оценки линейных форм

3.1. Разложение модульной $\mathcal{L}$-матрицы. Для столбцов $\widehat{\alpha}$ из (2.12) и $\widehat{\zeta}$ из (2.6) определим квадратные матрицы

$$A = (\widehat{\alpha}^{(1)} \ldots \widehat{\alpha}^{(d+1)}), \quad Z = (\widehat{\zeta}^{(1)} \ldots \widehat{\zeta}^{(d+1)}) \tag{3.1}$$

– порядка $d+1$. Матрица Z невырождена и в силу равенства (2.11) можем записать

$$A = TZ. \tag{3.2}$$

Поэтому матрица A также невырождена и, следовательно, ее столбцы образуют базис (A-базис) в пространстве $\mathbb{R}^{d+1}$.

Пусть P_α – модульная $\mathcal{L}$-матрица (2.17). Из равенства (2.18) получаем

$$\mathrm{P}_\alpha A \quad = (\lambda^{(1)}\widehat{\alpha}^{(1)} \ldots \lambda^{(d+1)}\widehat{\alpha}^{(d+1)}) \quad = A\Lambda,$$

где

$$\Lambda = \begin{pmatrix} \lambda^{(1)} & \dots & 0 \\ & \dots & \\ 0 & \dots & \lambda^{(d+1)} \end{pmatrix}. \tag{3.3}$$

Отсюда для матрицы P_α выводим разложение

$$\mathrm{P}_\alpha = A\Lambda A^{-1}. \tag{3.4}$$

3.2. Итерации целочисленных векторов. Определим векторы p_a для $a = 0, 1, 2, \dots$, записанные в виде столбцов

$$p_a = \begin{pmatrix} p_{a,1} \\ \vdots \\ p_{a,d+1} \end{pmatrix}, \tag{3.5}$$

через итерации

$$p_a = \mathrm{P}_\alpha p_{a-1}, \tag{3.6}$$

где p_0 – произвольный ненулевой целочисленный вектор. Повторяя (3.6) несколько раз, получаем

$$p_a = \mathrm{P}_\alpha^a p_0. \tag{3.7}$$

Из (3.3), (3.4) и (3.7) следует явное представление

$$p_a = \begin{pmatrix} {\lambda^{(1)}}^a a_{1,1} + \dots + {\lambda^{(d+1)}}^a a_{1,d+1} \\ \vdots \\ {\lambda^{(1)}}^a a_{d+1,1} + \dots + {\lambda^{(d+1)}}^a a_{d+1,d+1} \end{pmatrix} \tag{3.8}$$

с некоторыми коэффициентами a_{ij}, не зависящими от a. Отсюда выводим неравенства

$$|p_{a,i}| \leqslant |\lambda^{(1)}|^a |a_{i,1}| + \dots + |\lambda^{(d+1)}|^a |a_{i,d+1}| \tag{3.9}$$

для $i = 1, \dots, d+1$.

Лемма 3.1. *Пусть векторы p_a определены формулой* (3.7). *Тогда для них имеет место неравенство*

$$|p_a|_s \leqslant c_{\alpha,p_0}\, \lambda_{\max}^a \tag{3.10}$$

для всех $a = 0, 1, 2, \dots$ Здесь обозначили

$$|p_a|_s = |p_{a,1}| + \dots + |p_{a,d+1}| \tag{3.11}$$

– s-метрику в пространстве $\mathbb{R}^{d+1}$,

$$\lambda_{\max} = \max_{1 \leqslant i \leqslant d+1} |\lambda^{(i)}| \tag{3.12}$$

и c_{α,p_0} *– константу, не зависящую от номера итерации* a.

Доказательство. Непосредственно вытекает из неравенств (3.9). □

3.3. Линейные формы. Выделим в $\mathbb{R}^{d+1}$ подпространства

$$A_+,\ A_- \subset \mathbb{R}^{d+1}, \tag{3.13}$$

натянутые соответственно на векторы

$$\begin{array}{lll} \widehat{\alpha}^{(i_+)}, & \widehat{\alpha}_+^{(j_+)}, & \widehat{\alpha}_-^{(j_+)}, \\ \widehat{\alpha}^{(i_-)}, & \widehat{\alpha}_+^{(j_-)}, & \widehat{\alpha}_-^{(j_-)}, \end{array} \tag{3.14}$$

где

$$\widehat{\alpha}_+^{(j)} = \tfrac{1}{2}(\widehat{\alpha}^{(j)} + \overline{\widehat{\alpha}}^{(j)}), \quad \widehat{\alpha}_-^{(j)} = \tfrac{1}{2i}(\widehat{\alpha}^{(j)} - \overline{\widehat{\alpha}}^{(j)}). \tag{3.15}$$

Так как столбцы матрицы A из (3.1) образуют базис в пространстве $\mathbb{R}^{d+1}$, то векторы (3.14) являются базисами подпространств $A_+,\ A_-$ и они разлагают пространство $\mathbb{R}^{d+1}$ в прямую сумму

$$\mathbb{R}^{d+1} = A_+ \oplus A_-. \tag{3.16}$$

Обозначим через

$$A_+^{\perp} \subset \mathbb{R}^{d+1} \tag{3.17}$$

подпространство, ортогональное $A_+^{\perp}\ \perp A_+$ к A_+ относительно обычного (покоординатного) скалярного произведения.

От комплексной матрицы A перейдем к *вещественной матрице*

$$A_{\mathbb{R}} = (\ldots \widehat{\alpha}^{(i)} \ldots \widehat{\alpha}_+^{(j)} \widehat{\alpha}_-^{(j)} \ldots), \tag{3.18}$$

столбцы которой образуют базис вещественного пространства $\mathbb{R}^{d+1}$. Разложим вектор p_0 из (3.5) по этому базису

$$p_0 = A_{\mathbb{R}} \begin{pmatrix} x_1 \\ \vdots \\ x_{d+1} \end{pmatrix} = \ldots + x_i \widehat{\alpha}^{(i)} + \ldots + (\widehat{\alpha}_+^{(j)} \widehat{\alpha}_-^{(j)}) X_j + \ldots, \tag{3.19}$$

где $X_j = \begin{pmatrix} x_j \\ x_j' \end{pmatrix}$.

Если $\lambda^{(j)} = |\lambda^{(j)}|\,(\cos\varphi_j + i\sin\varphi_j)$, то по (3.7) находим

$$p_a = \mathrm{P}_\alpha^a\, p_0 = \ldots + x_i {\lambda^{(i)}}^a\, \widehat{\alpha}^{(i)} + \ldots + |\lambda^{(j)}|^a X_j(a\varphi_j) + \ldots, \tag{3.20}$$

где

$$X_j(a\varphi_j) = (\widehat{\alpha}_+^{(j)}\ \widehat{\alpha}_-^{(j)}) \begin{pmatrix} x_j(a\varphi_j) \\ x_j'(a\varphi_j) \end{pmatrix},$$

при этом

$$\begin{pmatrix} x_j(a\varphi_j) \\ x'_j(a\varphi_j) \end{pmatrix} = \begin{pmatrix} \cos(a\varphi_j) & -\sin(a\varphi_j) \\ \sin(a\varphi_j) & \cos(a\varphi_j) \end{pmatrix} \begin{pmatrix} x_j \\ x'_j \end{pmatrix}.$$

Из (3.17) и (3.20) для любого вектора $\alpha^\perp \in A_+^\perp$ имеем

$$p_a \cdot \alpha^\perp = \ldots + x_{i_-} \lambda^{(i_-)^a} \widehat{\alpha}^{(i_-)} \cdot \alpha^\perp + \ldots + |\lambda^{(j_-)}|^a X_{j_-}(a\varphi_{j_-}) \cdot \alpha^\perp + \ldots, \quad (3.21)$$

где

$$X_{j_-}(a\varphi_{j_-}) \cdot \alpha^\perp = (\widehat{\alpha}_+^{(j_-)} \cdot \alpha^\perp \quad \widehat{\alpha}_-^{(j_-)} \cdot \alpha^\perp) \begin{pmatrix} x_j(a\varphi_{j_-}) \\ x'_j(a\varphi_{j_-}) \end{pmatrix}. \quad (3.22)$$

Лемма 3.2. *Для любого вектора $\alpha^\perp \in A_+^\perp$ определим линейную форму*

$$F_{\alpha^\perp}(x) = \alpha_1^\perp x_1 + \ldots + \alpha_{d+1}^\perp x_{d+1} \quad (3.23)$$

с вещественными коэффициентами $\alpha_i^\perp$, равными координатам вектора $\alpha^\perp$. Тогда значение формы $F_{\alpha^\perp}(p_a)$ в точке p_a из (3.7) *оценивается как*

$$|F_{\alpha^\perp}(p_a)| \leqslant c_{\alpha,\alpha^\perp,p_0}\, \lambda_{\max_-}^a \quad (3.24)$$

с константой $c_{\alpha,\alpha^\perp,p_0}$, не зависящей от номера a, и $0 < \lambda_{\max_-} < 1$, определяемым равенством

$$\lambda_{\max_-} = \max_{1 \leqslant i_-, j_- \leqslant d+1} \{|\lambda^{(i_-)}|, |\lambda^{(j_-)}|\}. \quad (3.25)$$

Доказательство. Так как по определению (3.23) линейной формы $F_{\alpha^\perp}(x)$ можем записать

$$F_{\alpha^\perp}(p_a) = p_a \cdot \alpha^\perp, \quad (3.26)$$

то неравенство (3.24) вытекает из разложения (3.21), (3.22) для скалярного произведения $p_a \cdot \alpha^\perp$ в (3.26) и определения (3.25). □

Теорема 3.1. *Пусть $F_{\alpha^\perp}(x)$ – линейная форма* (3.23) *и целочисленные векторы p_a определяются формулой* (3.7). *Тогда выполняется неравенство*

$$|F_{\alpha^\perp}(p_a)| \leqslant \frac{C}{|p_a|_s^{1/\mu - \varrho}} \quad (3.27)$$

для всех $a = 0, 1, 2, \ldots$ Здесь $\frac{1}{d} \leqslant \mu \leqslant d$ вычисляется по формуле (2.16); *показатель ϱ удовлетворяет неравенствам*

$$0 < \varrho \leqslant C_\varepsilon \eta, \quad (3.28)$$

где константа $C_\varepsilon > 0$ *не зависит от параметра* η *из* (1.30), *который можно выбирать сколь угодно малым; константа* $C = C_{\alpha,\alpha^\perp,\eta,p_0}$ *не зависит от номера итерации* a.

Доказательство. Объединяя (1.28) и (2.19) можем записать

$$\begin{aligned} |\lambda^{(i_+)}| &= \lambda_+^{1+\theta_{i_+}}, \quad |\lambda^{(i_-)}| = \lambda_+^{-1/\mu+\theta_{i_-}}, \\ |\lambda^{(j_+)}| &= \lambda_+^{1+\theta_{j_+}}, \quad |\lambda^{(j_-)}| = \lambda_+^{-1/\mu+\theta_{j_-}}, \end{aligned} \tag{3.29}$$

где $\lambda_+ = \zeta_+^\nu > 1$ и показатели θ_i, θ_j удовлетворяют неравенствам (1.31). Из (3.25) и (3.29) получаем

$$\lambda_{\max_-} = \lambda_+^{-1/\mu-\theta_{\max_-}} \tag{3.30}$$

с показателем

$$\theta_{\max_-} = -\max_{1\leqslant i_-,j_-\leqslant d+1} \{\theta_{i_-}, \theta_{j_-}\} \tag{3.31}$$

и неравенство (3.24) примет вид

$$|F_{\alpha^\perp}(p_a)| \leqslant c_{\alpha,\alpha^\perp,p_0}\, \lambda_+^{-a(1/\mu+\theta_{\max_-})}. \tag{3.32}$$

С другой стороны, согласно (3.12) и (3.29) находим

$$\lambda_{\max} = \lambda_+^{1+\theta_{\max_+}}, \tag{3.33}$$

где

$$\theta_{\max_+} = \max_{1\leqslant i_+,j_+\leqslant d+1} \{\theta_{i_+}, \theta_{j_+}\}. \tag{3.34}$$

Поэтому подставляя (3.33) в (3.10), приходим к неравенству

$$|p_a|_s \leqslant c_{\alpha,p_0}\, \lambda_+^{a(1+\theta_{\max_+})}, \tag{3.35}$$

однородному с (3.32).

Теперь неравенство (3.27) следует из (3.32) и (3.35), а неравенство (3.28) из (1.31). □

§4. Оценка приближений систем линейных форм

4.1. Оценка снизу. Ранее в лемме 3.1 была получена верхняя оценка для $|p_a|_s$. Далее нам потребуется также и нижняя оценка.

Лемма 4.1. *Пусть векторы* p_a *определены формулой* (3.7). *Тогда для них имеет место неравенство*

$$|p_a|_s \geqslant c_{p_0,A}\, \lambda_{\min_+}^a \tag{4.1}$$

для всех $a = 0, 1, 2, \ldots,$ *где*

$$\lambda_{\min_+} = \min_{1 \leqslant i_+, j_+ \leqslant d+1} \{|\lambda^{(i_+)}|, |\lambda^{(j_+)}|\} > 1 \tag{4.2}$$

и константа $c_{p_0,A} > 0$ *не зависит от номера итерации* a.

Доказательство. Воспользуемся разложением (3.20) векторов p_a. Если в разложении (3.19) вектора p_0 все $x_{i_+} = 0$ и $X_{j_+} = 0$, то $p_a \to 0$ при $a \to \infty$. Но векторы p_a целочисленные, поэтому $p_a = 0$ для достаточно больших значений a и, следовательно, $p_0 = p_a \mathrm{P}_\alpha^{-a} = 0$ по формуле (3.7), что противоречит выбору $p_0 \neq 0$.

Пусть в разложении (3.19) существует $x_{i_+} \neq 0$. Тогда у векторов p_a из (3.20) модуль i_+-ой координаты

$$|x_{i_+} \lambda^{(i_+)^a}| = |x_{i_+}|\, \lambda^{(i_+)^a} \to \infty \quad \text{при} \quad a \to \infty. \tag{4.3}$$

Теперь предположим, что в разложении (3.19) найдется столбец $X_{j_+} = \begin{pmatrix} x_{j_+} \\ x'_{j_+} \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. Тогда

$$\min_{\substack{\varphi \in [0, 2\pi) \\ a = 1, 2, \ldots}} |X_{j_+}(a\varphi)| = \min_{\varphi \in [0, 2\pi)} |X_{j_+}(\varphi)| = c_{j_+} > 0,$$

и поэтому

$$||\lambda^{(j_+)}|^a X_{j_+}(a\varphi_{j_+})| \geqslant c_{j_+}\, |\lambda^{(j_+)}|^a \to \infty \quad \text{при} \quad a \to \infty. \tag{4.4}$$

Пусть $|{*}|_{s,A}$ обозначает s-метрику (3.11), записанную в базисе (3.18). Из разложения (3.20) и свойств (4.3), (4.4) вытекает

$$|p_a|_{s,A} \geqslant c'_{p_0,A}\, \lambda^a_{\min_+} \tag{4.5}$$

для всех $a = 0, 1, 2, \ldots$, где $\lambda_{\min_+} > 1$ определено в (4.2) и константа $c'_{p_0,A} > 0$ не зависит от номера итерации a. Поскольку s-метрики $|*|_s$ и $|*|_{s,A}$ эквивалентны – так как это одна и та же метрика в разных базисах – то из неравенства (4.5) будет следовать оценка (4.1). □

4.2. Рекуррентные последовательности. Из матричной итерационной формулы (3.6) выведем рекуррентную формулу для координат $p_a = \begin{pmatrix} p_{a,1} \\ \vdots \\ p_{a,d+1} \end{pmatrix}$ целочисленных точек (3.5). Пусть $\mathcal{L}$-матрица P_α имеет характеристический многочлен

$$ch_{\mathrm{P}_\alpha}(x) = \det(xE - \mathrm{P}_\alpha) = x^{d+1} - b_d x^d - \ldots - b_1 x - b_0. \tag{4.6}$$

В [9] было доказано следующее утверждение.

Предложение 4.1. *Столбцы p_a удовлетворяют рекуррентному соотношению*

$$p_{a+d+1} = b_d\, p_{a+d} + \ldots + b_1\, p_{a+1} + b_0\, p_a \tag{4.7}$$

для $a = 0, 1, 2, \ldots$ При этом начальные условия

$$p_d = \mathrm{P}_\alpha^d\, p_0, \ldots, \quad p_1 = \mathrm{P}_\alpha\, p_0, \quad p_0 \tag{4.8}$$

задаются $\mathcal{L}$-матрицей P_α из (2.17) *и столбцом p_0, определенным в* (3.6) *и* (3.7).

4.3. Основная теорема. Согласно (1.6) и (1.8) пространство $A_+^\perp$ из (3.17) имеет размерность, равную

$$k^\perp = \dim_{\mathbb{R}} A_+^\perp = d + 1 - k \tag{4.9}$$

Поэтому в силу (1.7) и (4.9) размерность $k^\perp$ пространства $A_+^\perp$ изменяется соответственно в границах

$$d \geqslant k^\perp \geqslant 1, \quad \text{где} \quad 1 \leqslant k \leqslant d. \tag{4.10}$$

Выберем в пространстве $A_+^\perp$ произвольный базис

$$\alpha_1^\perp = (\alpha_{1,1}^\perp, \ldots, \alpha_{1,d+1}^\perp), \quad \ldots, \quad \alpha_{k^\perp}^\perp = (\alpha_{k^\perp,1}^\perp, \ldots, \alpha_{k^\perp,d+1}^\perp) \tag{4.11}$$

и несколько упрощая правило (3.23) поставим базису (4.11) в соответствие *систему линейных форм*

$$\begin{aligned} F_1(x) &= \alpha_{1,1}^\perp x_1 + \ldots + \alpha_{1,d+1}^\perp x_{d+1}, \\ &\ldots \\ F_{k^\perp}(x) &= \alpha_{k^\perp,1}^\perp x_1 + \ldots + \alpha_{k^\perp,d+1}^\perp x_{d+1} \end{aligned} \tag{4.12}$$

с вещественными коэффициентами. Из определения следует, что линейные формы (4.12) образуют базис в пространстве $F_+^\perp$ всех линейных форм $F_{\alpha^\perp}(x)$, где $\alpha^\perp \in A_+^\perp$.

Теорема 4.1. *Пусть в пространстве $F_+^\perp$ задана некоторая система вещественных линейных форм* (4.12) *и целочисленные точки $p_a = (p_{a,1}, \ldots, p_{a,d+1})$ определяются рекуррентным соотношением* (4.7) *с начальными условиями* (4.8). *Тогда в обозначениях теоремы* 3.1 *справедливы следующие утверждения.*

1. *Выполняется система неравенств*

$$\begin{array}{c} |F_1(p_a)| \leqslant \frac{C}{|p_a|_s^{1/\mu-\varrho}}, \\ \dots \\ |F_{k^\perp}(p_a)| \leqslant \frac{C}{|p_a|_s^{1/\mu-\varrho}} \end{array} \tag{4.13}$$

для всех $a = 0, 1, 2, \dots$ *Здесь* $\mu = \frac{d-k+1}{k}$, *показатель* $\varrho > 0$ *можно выбрать сколь угодно малым и константа* C *не зависит от номера итерации* a.

2. *Величина* $|p_a|_s = |p_{a,1}| + \ldots + |p_{a,d+1}|$ *имеет экспоненциальный рост относительно номера* a.

Доказательство. Неравенства (4.13) вытекают из теоремы 3.1 и предложения 4.1. Согласно леммам 3.1 и 4.1 величина $|p_a|_s$ удовлетворяет неравенствам

$$c'\,\lambda^a_{\min_+} \leqslant |p_a|_s \leqslant c''\,\lambda^a_{\max} \tag{4.14}$$

с константами $c' > 0$, $c'' > 0$ и $1 < \lambda_{\min_+} \leqslant \lambda_{\max}$ по определениям (3.12) и (4.2). Из неравенств (4.14) следует второе утверждение теоремы. □

Алгоритм построения целочисленных решений $p_a = (p_{a,1}, \dots, p_{a,d+1})$ систем линейных неравенств вида (4.13), разработанный в п.п. 1-4, назовем *$\mathcal{L}$-алгоритмом.* Как мы видели, данный алгоритм опирается на метод локализации единиц $\mathcal{L}$ алгебраических числовых полей $\mathbb{F} = \mathbb{Q}(\theta)$, изложенный в п. 1.

§5. Пример линейных форм от четырех переменных

Покажем, как работает предложенный в п.п. 1–4 $\mathcal{L}$-алгоритм на примере аппроксимации линейной формы с вещественными алгебраическими коэффициентами четвертой степени.

5.1. Выбор локализованной единицы. Рассмотрим вещественное алгебраическое поле $\mathbb{F} = \mathbb{Q}(\sqrt[4]{2})$ степени $\deg \mathbb{F}/\mathbb{Q} = 4$, имеющее $r = 2$ вещественных и $2c = 2$ комплексных сопряжений. В нашем случае $d = 3$. Если выбрать $k = 3$, то по формуле (4.9) пространство $A_+^\perp$ из (3.17) имеет размерность

$$k^\perp = \dim_{\mathbb{R}} A_+^\perp = 1, \tag{5.1}$$

т.е. пространство линейных форм одномерно.

Проверим, что в качестве единицы (1.34) можно взять элемент

$$\zeta = \varepsilon - 1, \tag{5.2}$$

где $\varepsilon = \sqrt[4]{2}$. Сопряженными $\zeta^{(j)}$ для элемента (5.2) будут

$$\begin{aligned} &\zeta^{(1)} = \zeta = \varepsilon - 1, \quad \zeta^{(2)} = -\varepsilon - 1, \\ &\zeta^{(3)} = i \quad \varepsilon - 1, \quad \zeta^{(4)} = \overline{\zeta}^{(3)} = -i\,\varepsilon - 1. \end{aligned} \tag{5.3}$$

Здесь $i = +\sqrt{-1}$ – мнимая единица. Отсюда для элемента ζ находим его норму

$$\mathrm{Norm}_{\,\mathbb{F}/\mathbb{Q}}(\zeta) = \zeta^{(1)} \cdot \zeta^{(2)} \cdot \zeta^{(3)} \cdot \zeta^{(4)} = -(\varepsilon^2 - 1)(\varepsilon^2 + 1) = -1. \tag{5.4}$$

Сопряженные (5.3) имеют модули

$$|\zeta^{(1)}| = \zeta \approx 0.18 < 1, \ \ |\zeta^{(2)}| \approx 2.18 > 1, \ \ |\zeta^{(3)}| = |\zeta^{(4)}| \approx 1.55 > 1. \tag{5.5}$$

Количество сопряженных с модулем > 1 равно $k = 3$ и, следовательно, в силу (5.4) элемент ζ подходит на роль локализованной единицы (1.34).

5.2. Базис подпространства A_+. Для этого нам потребуется знать векторы

$$\widehat{\zeta}^{(i)} = \begin{pmatrix} \zeta^{(i)3} \\ \zeta^{(i)2} \\ \zeta^{(i)} \\ 1 \end{pmatrix} \tag{5.6}$$

высоты $d + 1 = 4$ для $i = 1, 2, 3, 4$. Используя явный вид сопряженных (5.3), вычисляем для векторов (5.6) их элементы

$$\begin{array}{lll} \zeta^{(1)3} = \varepsilon^3 - 3\varepsilon^2 + 3\varepsilon - 1, & \zeta^{(1)2} = \varepsilon^2 - 2\varepsilon + 1, & \zeta^{(1)} = \varepsilon - 1, \\ \zeta^{(2)3} = -\varepsilon^3 - 3\varepsilon^2 - 3\varepsilon - 1, & \zeta^{(2)2} = \varepsilon^2 + 2\varepsilon + 1, & \zeta^{(2)} = -\varepsilon - 1, \\ \zeta^{(3)3} = -i\varepsilon^3 - 3\varepsilon^2 + 3i\varepsilon - 1, & \zeta^{(3)2} = -\varepsilon^2 - 2i\varepsilon + 1, & \zeta^{(3)} = i\varepsilon - 1, \\ \zeta^{(4)3} = i\varepsilon^3 - 3\varepsilon^2 - 3i\varepsilon - 1, & \zeta^{(4)2} = -\varepsilon^2 + 2i\varepsilon + 1, & \zeta^{(4)} = -i\varepsilon - 1. \end{array} \tag{5.7}$$

Теперь найдем базис подпространства $A_+ \subset \mathbb{R}^4$ из (3.13), состоящий из $k = 3$ векторов

$$\widehat{\zeta}^{(2)}_+ = \begin{pmatrix} \zeta^{(2)3}_+ \\ \zeta^{(2)2}_+ \\ \zeta^{(2)}_+ \\ 1 \end{pmatrix}, \ \widehat{\zeta}^{(3)}_+ = \begin{pmatrix} \zeta^{(3)3}_+ \\ \zeta^{(3)2}_+ \\ \zeta^{(3)}_+ \\ 1 \end{pmatrix}, \ \widehat{\zeta}^{(3)}_- = \begin{pmatrix} \zeta^{(3)3}_- \\ \zeta^{(3)2}_- \\ \zeta^{(3)}_- \\ 0 \end{pmatrix}. \tag{5.8}$$

Используя (5.7), по формулам (3.14) и (3.15) вычисляем данные векторы в координатах

$$\widehat{\zeta}_{+}^{(2)} = \begin{pmatrix} -\varepsilon^3 - 3\varepsilon^2 - 3\varepsilon - 1 \\ \varepsilon^2 + 2\varepsilon + 1 \\ -\varepsilon - 1 \\ 1 \end{pmatrix}, \quad \widehat{\zeta}_{+}^{(3)} = \begin{pmatrix} 3\varepsilon^2 - 1 \\ -\varepsilon^2 + 1 \\ -1 \\ 1 \end{pmatrix},$$
$$\widehat{\zeta}_{-}^{(3)} = \begin{pmatrix} -\varepsilon^3 + 3\varepsilon \\ -2\varepsilon \\ \varepsilon \\ 0 \end{pmatrix}. \tag{5.9}$$

5.3. Нахождение линейной формы. Удобно начать с вычисления следующего векторного определителя

$$D_{\mathbf{e}} = \det \begin{pmatrix} \zeta_{+}^{(2)3} & \zeta_{+}^{(3)3} & \zeta_{-}^{(3)3} & \mathbf{e}_1 \\ \zeta_{+}^{(2)2} & \zeta_{+}^{(3)2} & \zeta_{-}^{(3)2} & \mathbf{e}_2 \\ \zeta_{+}^{(2)} & \zeta_{+}^{(3)} & \zeta_{-}^{(3)} & \mathbf{e}_3 \\ 1 & 1 & 1 & \mathbf{e}_4 \end{pmatrix}, \tag{5.10}$$

где

$$\mathbf{e}_1 = (1,0,0,0), \quad \mathbf{e}_2 = (0,1,0,0), \quad \mathbf{e}_3 = (0,0,1,0), \quad \mathbf{e}_4 = (0,0,0,1)$$

– единичный базис в $\mathbb{R}^4$. Согласно (5.1) пространство $A_{+}^{\perp}$ имеет размерность $k^{\perp} = 1$ и по определению (5.10) вектор $D_{\mathbf{e}} \in A_{+}^{\perp}$, поэтому данное пространство порождается вектором

$$\alpha^{\perp} = (\alpha_1^{\perp}, \alpha_2^{\perp}, \alpha_3^{\perp}, \alpha_4^{\perp}) = D_{\mathbf{e}}. \tag{5.11}$$

Вычисляя определитель (5.10), находим координаты этого вектора

$$\begin{array}{ll} \alpha_1^{\perp} = 2\varepsilon^3, & \alpha_2^{\perp} = 6\varepsilon^3 + 4, \\ \alpha_3^{\perp} = 6\varepsilon^3 + 4\varepsilon + 8, & \alpha_4^{\perp} = 2\varepsilon^3 + 4\varepsilon^2 + 4\varepsilon + 4. \end{array} \tag{5.12}$$

Используя (5.12), можем записать нужную нам линейную форму

$$F_{\alpha^{\perp}}(x) = \alpha_1^{\perp} x_1 + \alpha_2^{\perp} x_2 + \alpha_3^{\perp} x_3 + \alpha_4^{\perp} x_4, \tag{5.13}$$

образующую базис в пространстве всех линейных форм $F_{+}^{\perp}$.

5.4. Модульная $\mathcal{L}$-матрица. Чтобы избежать большого объема вычислений, в качестве $\widehat{\alpha}$ из (2.12) выберем вектор

$$\widehat{\alpha} = \widehat{\zeta}. \tag{5.14}$$

Тогда формула (2.18) примет вид

$$\mathrm{P}_\zeta \, \widehat{\zeta} = \lambda \cdot \widehat{\zeta}, \tag{5.15}$$

где согласно (5.5) собственное значение $\lambda = \zeta$ является $\mathcal{L}$-единицей из множества (2.1), а значит, матрица представления P_ζ будет модульной $\mathcal{L}$-матрицей. Вспоминая, что $\zeta = \varepsilon - 1$ и $\varepsilon = \sqrt[4]{2}$ (см. (5.2)), находим эту матрицу

$$\mathrm{P}_\zeta = \begin{pmatrix} -4 & -6 & -4 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{5.16}$$

5.5. Рекуррентное соотношение. Выведем рекуррентную формулу для координат

$$p_a = \begin{pmatrix} p_{a,1} \\ p_{a,2} \\ p_{a,3} \\ p_{a,4} \end{pmatrix} \tag{5.17}$$

целочисленных точек (3.5). Для этого нужно знать характеристический многочлен (4.6) для $\mathcal{L}$-матрицы P_ζ. Используя (5.16), получаем многочлен

$$ch_{\mathrm{P}_\zeta}(x) = x^4 + 4x^3 + 6x^2 + 4x - 1 \tag{5.18}$$

с коэффициентами $b_3 = -4$, $b_2 = -6$, $b_1 = -4$, $b_0 = 1$. Поэтому по предложению 4.1 столбцы (5.17) удовлетворяют рекуррентному соотношению

$$p_{a+4} = -4p_{a+3} - 6p_{a+2} - 4p_{a+1} + p_a \tag{5.19}$$

для $a = 0, 1, 2, \ldots$ Осталось найти начальные условия (4.8). Согласно (3.6), (3.7) столбец p_0 должен быть целочисленным и ненулевым. Если положить $p_0 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$, то в силу формул (4.8) начальными условиями будут следующие точки

$$p_0 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \ p_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \ p_2 = \begin{pmatrix} -4 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \ p_3 = \begin{pmatrix} 10 \\ -4 \\ 1 \\ 0 \end{pmatrix}. \tag{5.20}$$

5.6. Аппроксимация линейной формы $F_{\alpha^\perp}$. Применяя оценку (3.24), можем записать

$$|F_{\alpha^\perp}(p_a)| = |\alpha_1^\perp p_{a1} + \alpha_2^\perp p_{a2} + \alpha_3^\perp p_{a3} + \alpha_4^\perp p_{a4}| \leqslant c_{\alpha,\alpha^\perp,p_0}\, \lambda_{\max_-}^a, \tag{5.21}$$

при этом по определению (3.25) и равенствам (5.5) находим $\lambda_{\max_-} = |\zeta^{(1)}| = \zeta$, где $\zeta \approx 0.18 < 1$. Далее, вспоминая леммы 3.1 и 4.1, приходим к двойному неравенству

$$c_{p_0,A}\, \lambda_{\min_+}^a \leqslant |p_a|_s \leqslant c_{\alpha,p_0}\, \lambda_{\max}^a, \tag{5.22}$$

где $\lambda_{\max} = |\zeta^{(2)}| \approx 2.18 > 1$ и $\lambda_{\min_+} = |\zeta^{(3)}| \approx 1.55 > 1$ по формулам (3.12) и (4.2).

Теперь подставим неравенство (5.22) в (5.21) и получим оценку

$$|F_{\alpha^\perp}(p_a)| \leqslant \frac{C}{|p_a|_s^\theta} \tag{5.23}$$

с показателем

$$\theta = -\frac{\ln \lambda_{\max_-}}{\ln \lambda_{\max}} = -\frac{\ln \zeta}{\ln |\zeta^{(2)}|},$$

удовлетворяющим в силу (5.3) неравенству

$$\theta > 2.12. \tag{5.24}$$

Итак, мы оценили (5.23), скорость приближения линейной формы $F_{\alpha^\perp}(p_a)$, где целочисленные переменные p_a имеют экспоненциальный рост (5.22).

5.7. Корневая линейная форма $F_{\sqrt[4]{2}}$. Рассмотренную выше линейную форму $F_{\alpha^\perp}(x)$ можно преобразовать в более простую форму $F_{\sqrt[4]{2}}(x)$. С этой целью вместо коэффициентов $\alpha_i^\perp$ подставим в (5.13) их выражения (5.12) через степени корня $\varepsilon = \sqrt[4]{2}$. Получим тождество

$$F_{\alpha^\perp}(x) = F_{\sqrt[4]{2}}(x'), \tag{5.25}$$

где

$$F_{\sqrt[4]{2}}(x') = \sqrt[4]{8}\, x_1' + \sqrt{2}\, x_2' + \sqrt[4]{2}\, x_3' + x_4' \tag{5.26}$$

– новая форма от переменных x_i', связанных с x_i линейным целочисленным преобразованием

$$\begin{pmatrix} x_1' \\ x_2' \\ x_3' \\ x_4' \end{pmatrix} = M \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}, \quad \text{где} \quad M = \begin{pmatrix} 2 & 6 & 6 & 2 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 4 & 4 \\ 0 & 4 & 8 & 4 \end{pmatrix}. \tag{5.27}$$

Из (5.25)-(5.27) получаем равенство

$$F_{\alpha^\perp}(p_a) = F_{\sqrt[4]{2}}(p_a'), \tag{5.28}$$

при этом

$$p_a' = M p_a, \quad \text{где} \quad p_a' = \begin{pmatrix} p_{a1}' \\ p_{a2}' \\ p_{a3}' \\ p_{a4}' \end{pmatrix}. \tag{5.29}$$

Поскольку преобразование (5.29) линейное, то рекуррентное соотношение (5.19) сохраняется

$$p_{a+4}' = -4p_{a+3}' - 6p_{a+2}' - 4p_{a+1}' + p_a' \tag{5.30}$$

и для столбцов p_a', а начальные условия для них получаются из условий (5.20) тем же самым преобразованием (5.29):

$$p_0' = \begin{pmatrix} 2 \\ 4 \\ 4 \\ 4 \end{pmatrix}, \ p_1' = \begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \ p_2' = \begin{pmatrix} -2 \\ 0 \\ 0 \\ 4 \end{pmatrix}, \ p_3' = \begin{pmatrix} 2 \\ 0 \\ 4 \\ -8 \end{pmatrix}. \tag{5.31}$$

Предложение 5.1. *Пусть целочисленные переменные* p_a' *из* (5.29) *удовлетворяют рекуррентному соотношению* (5.30) *с начальными условиями* (5.31). *Тогда справедлива следующая оценка*

$$\left| \sqrt[4]{8}\, p_{a1}' + \sqrt{2}\, p_{a2}' + \sqrt[4]{2}\, p_{a3}' + p_{a4}' \right| \leqslant \frac{C'}{|p_a'|_s^\theta} \tag{5.32}$$

для всех $a = 1, 2, 3, \ldots$ *Здесь переменные* p_a' *имеют экспоненциальный рост возможно с другими константами в* (5.22), *показатель* $\theta = 2.12$ *и за константу в неравенстве* (5.32) *можно взять* $C' = 10^2$.

Доказательство. Так как матрица M преобразования (5.29) невырожденна и столбцы p_a, p_a' удовлетворяют одному и тому же рекуррентному соотношению (5.19), (5.30), то имеет место асимптотическая эквивалентность $|p_a'|_s \asymp |p_a|_s$ при $a \to +\infty$. Поэтому из оценки

(5.23), (5.24) и равенства (5.28) будет вытекать требуемое неравенство (5.32). □

Замечание 5.1. Соглано теореме 4.1 показатеть θ в неравенстве (5.32) можно подобрать сколь угодно близким к величине $\frac{1}{\mu}$, где $\mu = \frac{d-k+1}{k}$. В нашем случае $d = k = 3$ (см. п. 5.1), поэтому получаем $\frac{1}{\mu} = 3$, т.е. показатеть θ должен быть близким к 3, а не указанным выше $\theta = 2.12$. Такое расхождение объясняется выбором простейшей $\mathcal{L}$-единицы $\zeta = \sqrt[4]{2} - 1$ в (5.2), модули сопряженных которой $\zeta^{(i)}$ имеют значения (5.5).

Список литературы

1. В. Шмидт, *Диофантовы приближения.* М., Мир, 1983.
2. В. Г. Журавлев, *Ядерные цепные дроби.* Владимир, ВлГУ, 2019.
3. В. Г. Журавлев, *Локализованные единицы Пизо и совместные приближения алгебраических чисел.* — Зап. научн. семин. ПОМИ **458** (2017), 104–134.
4. В. Г. Журавлев, *Диофантовы приближения линейных форм.* — Зап. научн. семин. ПОМИ (2020), 1–18. (в печати)
5. T.W. Cusick, *Diophantine Approximation of Ternary Linear Forms.* — Math. Comp. **25** (1971), To. 113, 163–180.
6. T.W. Cusick, *Diophantine Approximation of Ternary Linear Forms. II.* — Math. Comp. **26** (1972), No. 120, 977–993.
7. З. И. Боревич, И. Р. Шафаревич, *Теория чисел.* Третье изд. М., Наука, 1985.
8. Журавлев В. Г., *Симплекс-ядерный алгоритм разложения в многомерные цепные дроби.* — Современные проблемы математики, МИАН **299** (2017), 1–20.
9. В. Г. Журавлев, *Симплекс-модульный алгоритм разложения алгебраических чисел в многомерные цепные дроби.* — Зап. научн. семин. ПОМИ **449** (2016), 168–195.

Zhuravlev V. G. $\mathcal{L}$-algorithm for approximating Diophantine systems of linear forms.

It is proposed $\mathcal{L}$ - algorithm for constructing an infinite sequence of integer solutions of linear inequality systems of $d+1$ variable. Solutions are obtained using recurrence relations of order $d+1$. The approach speed is carried out with the diophantine exponent $\theta = \frac{m}{n} - \varrho$ where $1 \leqslant n \leqslant d$ is the number of inequalities, $m = d+1-n$ — the number of free variables and the deviation $\varrho > 0$ can be made arbitrarily small due to a suitable choice of the recurrence relation.

Владимирский государственный университет
600024, Владимир, Строителей, 11, Россия
E-mail: vzhuravlev@mail.ru

Поступило 24 марта 2020 г.