1 Элиминация кванторов в упорядоченном поле вещественных чисел

Возьмём в качестве σ сигнатуру упорядоченных полей, т.е.

$$\sigma \;:=\; \langle 0, 1; +^2, -^1, \cdot^2; <^2, =^2 \rangle.$$

Обозначим через $\mathfrak{R}$ стандартную σ-структуру с носителем $\mathbb{R}$. Наша цель — показать, что $\mathrm{Th}\,(\mathfrak{R})$ допускает элиминацию кванторов.

Говорят, что $S \subseteq \mathbb{R}^n$ является *полиномиальным* (или *полуалгебраическим*), если S определимо в $\mathfrak{R}$ посредством некоторой бескванторной σ-формулы. Возьмём

$$\mathcal{P}_n \;:=\; \{S \subseteq \mathbb{R}^n \mid S \text{ полиномиально}\}.$$

Для удобства обозначим объединение $\{\mathcal{P}_n \mid n \in \mathbb{N}\}$ через $\mathcal{P}$. Как можно легко убедиться, следующие утверждения эквивалентны:

i. $\mathrm{Th}\,(\mathfrak{R})$ допускает элиминацию кванторов;

ii. проекция полиномиального множества полиномиальна.

Пункт (ii) можно ещё переформулировать так: $\mathcal{P}$ замкнуто относительно проекций.

Рассмотрим расширенную сигнатуру

$$\sigma^* \;:=\; \sigma \cup \bigcup_{\ell \in \mathbb{N}_+} \{\underline{f} \mid f : \mathbb{R}^\ell \to \mathbb{R}\},$$

где $\underline{f}$ суть новые функциональные символы. Обозначим через $\mathfrak{R}^*$ стандартную σ^*-структуру с носителем $\mathbb{R}$. Мы будем называть $f : \mathbb{R}^\ell \to \mathbb{R}$ *хорошей*, если существует алгоритм, который по любым $\Psi \in \mathrm{Form}_\sigma^\circ$ и $x \in \mathrm{Var}$ строит $\Psi_{(x,f)} \in \mathrm{Form}_\sigma^\circ$ такую, что

$$\mathrm{Th}\,(\mathfrak{R}^*) \vdash \Psi_{(x,f)} \leftrightarrow \Psi\left(x/\underline{f}\,(u_1, \ldots, u_\ell)\right),$$

где $u_1, \ldots, u_\ell$ попарно различны и не входят в Ψ. В дальнейшем мы будем часто писать f вместо $\underline{f}$. Разумеется, если $p\,(x_1, \ldots, x_\ell) \in \mathbb{Q}\,[x_1, \ldots, x_\ell]$, то $\lambda \vec{x}.\, [p\,(\vec{x})]$ хороша.

Лемма 1.1

Композиция хороших функций хороша. Точнее, пусть

$$h : \mathbb{R}^n \to \mathbb{R}, \quad g_1 : \mathbb{R}^\ell \to \mathbb{R}, \quad \ldots, \quad g_n : \mathbb{R}^\ell \to \mathbb{R}$$

хороши. Тогда $f : \mathbb{R}^\ell \to \mathbb{R}$, заданная по правилу

$$f\,(\vec{r}) \;:=\; h\,(g_1\,(\vec{r}), \ldots, g_n\,(\vec{r})),$$

также хороша.

Доказательство. Пусть $\Psi \in \mathrm{Form}_\sigma^\circ$ и $x \in \mathrm{Var}$. Так как h хороша, мы можем эффективно найти $\Theta_0 \in \mathrm{Form}_\sigma^\circ$ такую, что

$$\mathrm{Th}\,(\mathfrak{R}^*) \vdash \Psi\,(x/h\,(y_1, \ldots, y_n)) \leftrightarrow \Theta_0.$$

Далее, поскольку g_1 хороша, можно построить $\Theta_1 \in \mathrm{Form}_\sigma^\circ$ такую, что

$$\mathrm{Th}\,(\mathfrak{R}^*) \vdash \Theta_1 \leftrightarrow \Theta_0\,(y_1/g_1\,(\vec{u})).$$

Продолжая этот процесс, мы сможем получить $\Theta_2, \Theta_3, \ldots, \Theta_n \in \mathrm{Form}_\sigma^\circ$ такие, что

$$\mathrm{Th}\,(\mathfrak{R}^*) \vdash \Theta_k \leftrightarrow \Theta_{k-1}\,(y_k/g_k\,(\vec{u})) \quad \text{для всех} \;\; k \in \{2, 3, \ldots, n\}.$$

При этом, как легко убедиться,

$$\mathrm{Th}\,(\mathfrak{R}^*) \vdash \Theta_n \leftrightarrow \Psi\,(x/\underbrace{h\,(g_1\,(\vec{u}), \ldots, g_n\,(\vec{u}))}_{f(\vec{u})}).$$

Очевидно, Θ_n вычисляется эффективно по Ψ и x. □

Лемма 1.2

Пусть S_1, …, S_n полиномиальны и образуют разбиение $\mathbb{R}^\ell$, а

$$g_1 : \mathbb{R}^\ell \to \mathbb{R}, \quad \ldots, \quad g_n : \mathbb{R}^\ell \to \mathbb{R}$$

хороши. Тогда $f : \mathbb{R}^\ell \to \mathbb{R}$, заданная по правилу

$$f\,(\vec{r}) \;:=\; \begin{cases} g_1\,(\vec{r}) & \text{если} \;\; \vec{r} \in S_1 \\ \ldots & \\ g_n\,(\vec{r}) & \text{если} \;\; \vec{r} \in S_n, \end{cases}$$

также хороша.

Доказательство. Зафиксируем какие-нибудь бескванторные σ-формулы

$$\Theta_1\,(\vec{u}), \quad \ldots, \quad \Theta_n\,(\vec{u}),$$

определяющие в $\mathfrak{R}$ соответственно S_1, …, S_n. Пусть $\Psi \in \mathrm{Form}_\sigma^\circ$ и $x \in \mathrm{Var}$. Тогда

$$\mathrm{Th}\,(\mathfrak{R}^*) \vdash \Psi\,(x/f\,(\vec{u})) \leftrightarrow \bigvee_{i=1}^{n} \Theta_i\,(\vec{u}) \wedge \Psi\,(x/g_i\,(\vec{u})).$$

Очевидно, выражение в правой части эквивалентности можно эффективно превратить в бескванторную σ-формулу. □

Пример. Функция sgn («сигнум») хороша. Кроме того, для всякого $p\,(x_1, \ldots, x_\ell) \in \mathbb{Q}\,[x_1, \ldots, x_\ell]$ функция $\lambda\vec{x}.\,[\mathrm{sgn}\,(p\,(\vec{x}))]$ хороша.

Для $k \in \mathbb{N}$ введём обозначение

$$\mathrm{p}_k\,(x; \overline{y}) \;:=\; \sum_{i=0}^{k} y_i \cdot x^i,$$

где $\overline{y}$ — сокращение для $(y_0, \ldots, y_k)$. Когда из контекста понятно, о каком именно k идёт речь, индекс $\cdot_k$ будет опускаться.

Лемма 1.3

$f : \mathbb{R}^\ell \to \mathbb{R}$ хороша, если и только если существует алгоритм, который по каждому $k \in \mathbb{N}$ выдаёт $\Psi_k(u_1, \ldots, u_\ell, \overline{y}) \in \mathrm{Form}^\circ_\sigma$ такую, что

$$\mathrm{Th}(\mathfrak{R}^*) \vdash \Psi_k(\vec{u}, \overline{y}) \leftrightarrow \mathrm{p}_k(f(\vec{u}); \overline{y}) > 0.$$

Доказательство. $\boxed{\Longrightarrow}$ Очевидно.

$\boxed{\Longleftarrow}$ Пусть $\Psi \in \mathrm{Form}^\circ_\sigma$ и $x \in \mathrm{Var}$. Используя аксиомы линейно упорядоченных полей, можно эффективно превратить Ψ в булеву комбинацию атомарных формул вида

$$\sum_{i=0}^{k} t_i \cdot x^i > 0,$$

где t_1, …, t_k не содержат x. Поэтому достаточно разобраться с такого рода атомарными формулами. Однако это просто, поскольку в $\mathrm{Th}(\mathfrak{R}^*)$:

$$\begin{aligned} \textstyle\sum_{i=0}^{k} t_i \cdot (f(\vec{u}))^i > 0 \quad &\longleftrightarrow \quad \mathrm{p}_k(f(\vec{u}); t_0, \ldots, t_k) > 0 \\ &\longleftrightarrow \quad \Psi_k(y_0/t_0) \ldots (y_k/t_k), \end{aligned}$$

где Ψ_k строится эффективно по k. □

Рассмотрим функцию div из $\mathbb{R}^2$ в $\mathbb{R}$, действующую по правилу

$$\mathrm{div}(r_1, r_2) \ := \begin{cases} r_1/r_2 & \text{если } r_2 \neq 0 \\ 0 & \text{иначе.} \end{cases}$$

Иными словами, div — это просто $\lambda x.\lambda y.\,[x/y]$, которая доопределена нулём.

Лемма 1.4

div хороша.

Доказательство. Пусть $k \in \mathbb{N}$. Тогда в $\mathrm{Th}(\mathfrak{R}^*)$:

- если $v^n > 0$, то мы имеем

$$\begin{aligned} \mathrm{p}_k(\mathrm{div}(u, v); \overline{y}) > 0 \quad &\longleftrightarrow \quad v^n \cdot \sum_{i=0}^{k} y_i \cdot \mathrm{div}(u, v)^i > 0 \\ &\longleftrightarrow \quad \sum_{i=0}^{k} y_i \cdot u^i \cdot v^{n-i} > 0; \end{aligned}$$

- если $v^n < 0$, то $\mathrm{p}_k(\mathrm{div}(u, v); \overline{y}) > 0$ равносильно $\sum_{i=0}^{k} y_i \cdot u^i \cdot v^{n-i} < 0$;
- если $v^n = 0$, то $\mathrm{p}_k(\mathrm{div}(u, v); \overline{y}) > 0$ равносильно $\mathrm{p}_k(0; \overline{y}) > 0$.

В силу предыдущих двух лемм, div хороша. □

Для каждого $k \in \mathbb{N}$ рассмотрим $\deg_k : \mathbb{R}^{k+1} \to \mathbb{N}$, действующую по правилу

$$\deg_k(r_0, \ldots, r_k) \;:=\; \begin{cases} \max\{i \mid r_i \neq 0\} & \text{если } \{i \mid r_i \neq 0\} \neq \varnothing \\ -1 & \text{иначе;} \end{cases}$$

иными словами, $\deg_k(\overline{r})$ — это степень $\mathrm{p}_k(x; \overline{r})$.

Лемма 1.5

$\deg_k$ хороша для любого $k \in \mathbb{N}$. $\square$

Пусть $\boldsymbol{f} : \mathbb{R}^\ell \to \mathbb{R}^n$. Разумеется, по $\boldsymbol{f}$ однозначно строятся функции $f_1, \ldots, f_n$ из $\mathbb{R}^\ell$ в $\mathbb{R}$ такие, что для любого $\vec{r} \in \mathbb{R}^\ell$,

$$\boldsymbol{f}(\vec{r}) \;=\; (f_0(\vec{r}), \ldots, f_n(\vec{r})).$$

Мы будем говорить, что $\boldsymbol{f}$ *хороша*, если $f_1, \ldots, f_n$ хороши.

Лемма 1.6

Для каждого $k \in \mathbb{N}$ найдутся хорошие

$$\boldsymbol{f} :\; \mathbb{R}^{k+1} \times \mathbb{R}^{k+1} \to \mathbb{R}^{k+1} \quad \text{и} \quad \boldsymbol{g} :\; \mathbb{R}^{k+1} \times \mathbb{R}^{k+1} \to \mathbb{R}^{k+1}.$$

такие, что в $\mathrm{Th}(\mathfrak{R}^*)$: если $\deg(\overline{z}) \geqslant 0$, то

$$\mathrm{p}(x; \overline{y}) \;=\; \mathrm{p}(x; \boldsymbol{f}(\overline{y}, \overline{z})) \cdot \mathrm{p}(x; \overline{z}) \;+\; \mathrm{p}(x; \boldsymbol{g}(\overline{y}, \overline{z})),$$

причём $\deg(\boldsymbol{g}(\overline{y}, \overline{z})) < \deg(\overline{z})$.

Доказательство. Индукция по k.

Для краткости положим

$$p \;:=\; \mathrm{p}(x; \overline{y}) \quad \text{и} \quad q \;:=\; \mathrm{p}(x; \overline{z}).$$

Отныне давайте считать, что $\deg(\overline{z}) \geqslant 0$.

- Пусть $k = 0$. Тогда $p = y_0$ и $q = z_0$. Поэтому мы можем взять

  $$\boldsymbol{f}(\overline{y}, \overline{z}) \;:=\; \frac{y_0}{z_0} \quad \text{и} \quad \boldsymbol{g}(\overline{y}, \overline{z}) \;:=\; 0,$$

  где y_0/z_0 отождествляется с $\mathrm{div}(y_0, z_0)$.[1]

- Пусть $k > 0$. Предположим, что $\deg(\overline{z}) = n$, где $n \in \{0, \ldots, k\}$. Заметим, что

  $$\begin{aligned} p \;&=\; \frac{y_k}{z_n} \cdot x^{k-n} \cdot q + \left(p - \frac{y_k}{z_n} \cdot x^{k-n} \cdot q\right) \\ &=\; \frac{y_k}{z_n} \cdot x^{k-n} \cdot q + \left(\sum_{i=0}^{k} y_i \cdot x^i - \sum_{i=0}^{n} \frac{y_k}{z_n} \cdot x^{k-n} \cdot z_i \cdot x^i\right) \\ &=\; \frac{y_k}{z_n} \cdot x^{k-n} \cdot q + \left(\sum_{i=0}^{k} y_i \cdot x^i - \sum_{i=0}^{n} \frac{y_k}{z_n} \cdot z_i \cdot x^{k-n+i}\right) \\ &=\; \frac{y_k}{z_n} \cdot x^{k-n} \cdot q + \left(\sum_{i=0}^{k-1} y_i \cdot x^i - \sum_{i=0}^{n-1} \frac{y_k}{z_n} \cdot z_i \cdot x^{k-n+i}\right). \end{aligned}$$

  Если $n = k$, то второе слагаемое — это остаток от деления p на q. Если же $n < k$, то второе слагаемое можно поделить на q, используя индукционную гипотезу.

□

[1] В частности, $y_0/0 = 0$.

Для удобства в дальнейшем мы будем считать, что у полиномов с нулевыми коэффициентами корней нет.

Лемма 1.7: основная

Для каждого $k \in \mathbb{N}$ найдутся хорошие

$$\eta_1 : \mathbb{R}^{k+1} \to \mathbb{R}, \quad \ldots, \quad \eta_k : \mathbb{R}^{k+1} \to \mathbb{R} \quad \text{и} \quad \mu : \mathbb{R}^{k+1} \to k+1$$

такие, что в $\mathrm{Th}\,(\mathfrak{R}^*)$:

- $\mu\,(\overline{y})$ равно числу различных корней $\mathrm{p}\,(x; \overline{y})$;
- $\eta_1\,(\overline{y}), \ldots, \eta_{\mu(\overline{y})}\,(\overline{y})$ суть все корни $\mathrm{p}\,(x; \overline{y})$, причём $\eta_1\,(\overline{y}) < \ldots < \eta_{\mu(\overline{y})}\,(\overline{y})$.

Доказательство. Индукция по k.

Пусть $k = 0$. Тогда $\mathrm{p}\,(x; \overline{y}) = y_0$, а потому $\mu\,(\overline{y}) = 0$.

Пусть $k > 0$. Рассмотрим

$$\mathrm{p}'\,(x; \overline{y}) \;:=\; y_1 + 2y_2 + \cdots + k y_k x^{k-1}.$$

В силу индукционной гипотезы, для $k-1$ можно найти соответствующие хорошие функции; обозначим их через $\xi_1, \ldots, \xi_{k-1}$ и ν. Возьмём

$$\kappa\,(\overline{y}) \;:=\; \nu\,(y_1, 2y_2, \ldots, k y_k) \quad \text{и} \quad \theta_i\,(\overline{y}) \;:=\; \xi_i\,(y_1, 2y_2, \ldots, k y_k),$$

где i пробегает $\{1, \ldots, k-1\}$. Для краткости мы будем порой опускать упоминание $\overline{y}$.

a. Пусть $\mathrm{p}'\,(x; \overline{y})$ — нулевой многочлен. Тогда $\mathrm{p}\,(x; \overline{y})$ равно y_0 и не имеет корней.

b. Пусть $\mathrm{p}'\,(x; \overline{y})$ — ненулевой многочлен, причём $\kappa\,(\overline{y}) = 0$. Тогда $\deg\,(\overline{y})$ нечётно (так как иначе $\kappa\,(\overline{y}) \neq 0$), а потому у $\mathrm{p}\,(x; \overline{y})$ есть ровно один корень.

c. Пусть $\mathrm{p}'\,(x; \overline{y})$ — ненулевой многочлен, причём $\kappa\,(\overline{y}) \neq 0$. Тогда $\mathrm{p}\,(x; \overline{y})$ как функция от x на каждом из интервалов

$$(-\infty, \theta_1), \quad (\theta_1, \theta_2), \quad \ldots, \quad (\theta_{\kappa-1}, \theta_\kappa), \quad (\theta_\kappa, +\infty)$$

монотонна, а значит, имеет не более одного корня. Кроме того, сами θ_i могут быть корнями $\mathrm{p}\,(x)$. Стало быть, число корней легко посчитать:

- если $\mathrm{p}'\,(\theta_1 - 1) \cdot \mathrm{p}\,(\theta_1) > 0$, то у $\mathrm{p}\,(x)$ на $(-\infty, \theta_1)$ есть один корень;
- если $\mathrm{p}\,(\theta_i) \cdot \mathrm{p}\,(\theta_{i+1}) < 0$, где $i \leqslant \kappa - 1$, то у $\mathrm{p}\,(x)$ на (θ_i, θ_{i+1}) есть один корень;
- если $\mathrm{p}'\,(\theta_\kappa + 1) \cdot \mathrm{p}\,(\theta_\kappa) < 0$, то у $\mathrm{p}\,(x)$ на $(\theta_\kappa, +\infty)$ есть один корень;
- если $\mathrm{p}\,(\theta_i) = 0$, то θ_i является корнем $\mathrm{p}\,(x)$, разумеется.

С помощью разбора случаев теперь уже нетрудно убедиться, что $\mu : \mathbb{R}^{k+1} \to k+1$, выдающая число различных корней $\mathrm{p}\,(x; \overline{y})$ для данных $\overline{y}$, является хорошей.

Осталось проверить, что в каждом из интервалов, где корень есть, этот корень можно задать посредством хорошей функции. (Расположить же все имеющиеся корни в порядке возрастания не составляет труда.) Мы ограничимся разбором частного случая:

$$\kappa\,(\overline{y}) \geqslant 2 \quad \text{и} \quad \mathrm{p}\,(\theta_1\,(\overline{y}); \overline{y}) \cdot \mathrm{p}\,(\theta_2\,(\overline{y}); \overline{y}) < 0. \tag{$*$}$$

Рассмотрим $\eta : \mathbb{R}^{k+1} \to \mathbb{R}$, действующую по правилу

$$\eta(\overline{r}) \;:=\; \begin{cases} \text{корень } \mathrm{p}(x;\overline{r}) \text{ на } (\theta_1(\overline{r}), \theta_2(\overline{r})) & \text{если } (*) \\ 0 & \text{иначе.} \end{cases}$$

Хочется показать, что η хороша. Для этого нужно найти алгоритм, который по каждому $m \in \mathbb{N}$ выдаёт $\Psi(\overline{y}, \overline{z}) \in \mathrm{Form}^\circ_\sigma$ такую, что

$$\mathrm{Th}(\mathfrak{R}^*) \vdash \Psi(\overline{y}, \overline{z}) \leftrightarrow ((*) \wedge \mathrm{p}_m(\eta(\overline{y}); \overline{z}) > 0).$$

Очевидно, $\mathrm{p}_m(\,\cdot\,; \overline{z})$ можно заменить здесь на остаток от деления $\mathrm{p}_m(\,\cdot\,; \overline{z})$ на $\mathrm{p}(\,\cdot\,; \overline{y})$, или точнее, $\mathrm{p}_k(\,\cdot\,; \overline{y})$. Поэтому, не ограничивая общности, положим $m = k - 1$; вместо p_{k-1} мы будем писать q, чтобы не путать p_{k-1} с p. Теперь рассмотрим интервалы

$$(-\infty, \xi_1(\overline{z})), \quad (\xi_1(\overline{z}), \xi_2(\overline{z})), \quad \ldots, \quad \big(\xi_{\nu(\overline{z})-1}(\overline{z}), \xi_{\nu(\overline{z})}(\overline{z})\big), \quad \big(\xi_{\nu(\overline{z})}(\overline{z}), +\infty\big)$$

На каждом из них $\mathrm{q}(x; \overline{z})$ не меняет знака. Стало быть, достаточно понять, где находится $\eta(\overline{y})$. Это можно сделать следующим образом.

a. Сначала определяем точное расположение $\theta_1(\overline{y})$ и $\theta_2(\overline{y})$ относительно

$$\xi_1(\overline{z}), \quad \ldots, \quad \xi_{\nu(\overline{z})}(\overline{z}).$$

b. Если между $\theta_1(\overline{y})$ и $\theta_2(\overline{y})$ не находится никакое из $\xi_1(\overline{z})$, …, $\xi_{\nu(\overline{z})}(\overline{z})$, то положение $\eta(\overline{y})$ легко определяется.

c. Пусть между $\theta_1(\overline{y})$ и $\theta_2(\overline{y})$ находятся $\xi_i(\overline{z})$, …, $\xi_j(\overline{z})$, где $i < j \leqslant \nu(\overline{z})$.

- Если среди $\xi_i(\overline{z})$, …, $\xi_j(\overline{z})$ есть корень $\mathrm{p}(x; \overline{y})$, то этот корень — $\eta(\overline{y})$.
- Если среди $\xi_i(\overline{z})$, …, $\xi_j(\overline{z})$ нет корней $\mathrm{p}(x; \overline{y})$, то $\eta(\overline{y})$ находится между соседними элементами в

$$\theta_1(\overline{y}), \quad \xi_i(\overline{y}), \quad \ldots, \quad \xi_j(\overline{y}), \;\; \theta_2(\overline{y}),$$

  на которых $\mathrm{p}(x; \overline{y})$ меняет знак.

В итоге мы поймём, где располагается $\eta(\overline{y})$ и определим знак $\mathrm{q}(\eta(\overline{y}); \overline{z})$.

Остальные случаи разбираются аналогичным образом. $\square$

Теорема 1.8

$\mathrm{Th}\,(\mathfrak{R})$ допускает эффективную элиминацию кванторов.

Доказательство. Рассмотрим σ-формулу

$$\Phi \;=\; \exists x\, \Psi,$$

где $\Psi \in \mathrm{Form}^{\circ}_{\sigma}$. Нужно построить $\rho\,(\Phi) \in \mathrm{Form}^{\circ}_{\sigma}$ такую, что

$$\mathrm{Th}\,(\mathfrak{R}) \vdash \Phi \leftrightarrow \rho\,(\Phi) \quad \text{и} \quad \mathrm{FV}\,(\rho\,(\Phi)) \;\subseteq\; \mathrm{FV}\,(\Phi).$$

Обозначим за $\mathrm{Term}^{-x}_{\sigma}$ множество всех σ-термов, в которые не входит x.

Для начала выпишем все атомарные подформулы Ψ:

$$\Omega_0, \quad \Omega_1, \quad \ldots, \quad \Omega_n.$$

Без ограничения общности будем считать, что каждая Ω_i имеет вид

$$t_{i,0} \;+\; t_{i,1}x \;+\; \ldots \;+\; t_{i,k_i}x^{k_i} \;>\; 0,$$

где $k_i \in \mathbb{N}$ и $\{t_{i,0}, \ldots, t_{i,k_i}\} \subseteq \mathrm{Term}^{-x}_{\sigma}$. Более того, мы можем считать, что

$$k_0 \;=\; k_1 \;=\; \ldots \;=\; k_n;$$

поэтому нижний индекс у k будет опускаться. Для удобства положим

$$\overline{t_i} \;:=\; (t_{i,0}, \ldots, t_{i,k}).$$

В силу основной леммы, найдутся хорошие

$$\eta_1 : \mathbb{R}^{k+1} \to \mathbb{R}, \;\; \ldots, \;\; \eta_k : \mathbb{R}^{k+1} \to \mathbb{R} \quad \text{и} \quad \mu : \mathbb{R}^{k+1} \to k+1,$$

обладающие соответствующими свойствами. Значит,

$$\eta_1\left(\overline{t_i}\right), \quad \ldots, \quad \eta_{\mu\left(\overline{t_i}\right)}\left(\overline{t_i}\right)$$

суть все корни полинома для Ω_i. Далее, используя разбор случаев, расположим все корни полиномов для Ω_0, …, Ω_n в порядке возрастания:

$$\lambda_1 \;<\; \ldots \;<\; \lambda_\ell.$$

(Здесь ℓ и все λ_j представляются посредством хороших функций.) Возьмём

$$\begin{aligned} T \;:=\; & \{\lambda_1 - 1, \lambda_\ell + 1\} \cup \\ & \{\mathrm{div}\,(\lambda_j + \lambda_{j+1}, 2) \mid 1 \leqslant j \leqslant \ell - 1\} \cup \\ & \{\lambda_j \mid 1 \leqslant j \leqslant \ell\}. \end{aligned}$$

Непосредственно проверяется, что

$$\mathrm{Th}\,(\mathfrak{R}^*) \vdash \exists x\, \Psi \leftrightarrow \left(\Psi\,(x/0) \vee \bigvee_{t \in T} \Psi\,(x/t)\right).$$

Стало быть, бескванторная σ-формула, получающаяся из правой части этой эквивалентности путём элиминации всех символов хороших функции, окажется искомой.

Аккуратный анализ показывает вычислимость описанной процедуры. $\square$

Следствие 1.9

$\mathrm{Th}\,(\mathfrak{R})$ разрешима.

Доказательство. Достаточно заметить, что $\mathrm{Th}\,(\mathfrak{R}) \cap \mathrm{Form}^{\circ}_{\sigma}$ разрешимо. $\square$

Следствие 1.10

Проекция полуалгебраического (над $\mathbb{R}$) множества полуалгебраична (над $\mathbb{R}$). $\square$

Доказательство. Очевидно, взятие проекции множества прямо соответствует навешиванию квантора существования на определяющую это множество формулу. $\square$

%можно сравнить с тем, что происходит в $\mathfrak{N}$

Обозначим через RCF множество, состоящее из аксиом линейно упорядоченных полей, σ-предложения

$$\forall x\,(0 < x \to \exists u\, x = u \cdot u),$$

а также всех σ-предложений вида

$$\forall \overline{u}\,(u_n \neq 0 \to \exists x\, \mathrm{p}_n\,(x; \overline{u}) = 0),$$

где n нечётно. Модели RCF называют *вещественно замкнутыми полями.*

Упражнение: непростое

Для любого линейно упорядоченного поля $\mathfrak{F}$ следующие условия эквивалентны:

i. $\mathfrak{F}$ вещественно замкнуто;

ii. в $\mathfrak{F}$ истинно $\forall x\,(0 < x \to \exists u\, u \cdot u = x)$, а также все σ-предложения вида

$$\forall x\, \forall y\, \forall \overline{u}\,(x < y \wedge \mathrm{p}_n\,(x; \overline{u}) \cdot \mathrm{p}_n\,(y; \overline{u}) < 0 \to \exists z\,(x < z < y \wedge \mathrm{p}_n\,(z; \overline{u}) = 0)),$$

которые представляют собой *полиномиальную версию теоремы о среднем значении.*

Отсюда получается альтернативная аксиоматизация класса всех вещественно замкнутых полей. Можно убедиться, что дедуктивное замыкание каждой из эти аксиоматизаций совпадает с $\mathrm{Th}\,(\mathfrak{R})$, в силу элиминации кванторов.

Замечание. На самом деле, в доказательстве теоремы 1.8 вместо $\mathfrak{R}$ мы могли бы использовать произвольное вещественно замкнутое поле.