



Hilbertov Nullstellensatz IV

– Uvod u teoriju modela –

Slavko Moconja

MATF

23.12.2025.

Hilbertov Nullstellensatz

Neka je F algebarski zatvoreno polje, i $R = F[X_1, \dots, X_n]$.

HN₁. Za $I \triangleleft R$, $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$.

HN₂. Za $I \triangleleft R$, $I \neq R$, $\mathbb{V}(I) \neq \emptyset$.

HN₃. Ako $f_1, \dots, f_m \in R$ ne generišu R postoji $\bar{a} \in F^n$ tako da $f_i(\bar{a}) = 0$ za sve $i = 1, \dots, m$.

- $\mathbb{V}(I) = \{\bar{a} \in F^n : (\forall f \in I) f(\bar{a}) = 0\}$;
- $\mathbb{I}(V) = \{f \in R : (\forall \bar{a} \in V) f(\bar{a}) = 0\}$;
- $\sqrt{I} = \{f \in R : (\exists k \geq 1) f^k \in I\}$.

Tvrđenje. HN₁, HN₂ i HN₃ su ekvivalentni.

Rabinovičev trik: $\text{HN}_3 \implies \text{HN}_1$

Neka je $I \triangleleft R$, $I \neq R$, $I = \langle f_1, \dots, f_m \rangle$, i $g \in \mathbb{I}(\mathbb{V}(I))$, $g \neq 0$.

U $F[X_1, \dots, X_n, Y]$ posmatrajmo polinome $f_1, \dots, f_m, 1 - Yg$; oni nemaju zajedničku nulu u F^{n+1} .

Prema HN_3 , postoje $\alpha_i(\overline{X}, Y), \beta(\overline{X}, Y) \in F[\overline{X}, Y]$ tako da:

$$\sum_{i=1}^m \alpha_i(\overline{X}, Y) f_i + \beta(\overline{X}, Y)(1 - Yg) = 1.$$

Za $Y = \frac{1}{g}$, dobijamo:

$$\sum_{i=1}^m \alpha_i(\overline{X}, \frac{1}{g}) f_i = 1.$$

Za dovoljno veliko k , $g^k \alpha_i(\overline{X}, \frac{1}{g}) \in R$, i:

$$g^k = \sum_{i=1}^m g^k \alpha_i(\overline{X}, \frac{1}{g}) f_i \in I.$$

Eliminacija kvantifikatora (QE)

Definicija. Neka je T $\mathcal{L}$ -teorija.

- a) Neka je $\varphi(\bar{v})$ $\mathcal{L}$ -formula. Kažemo da T *eliminise kvantifikatore u* $\varphi(\bar{v})$ ako postoji beskvantorna $\mathcal{L}$ -formula $\psi(\bar{v})$ takva da:

$$T \models \forall \bar{v} (\varphi(\bar{v}) \leftrightarrow \psi(\bar{v})).$$

- b) T *eliminise kvantifikatore* ako eliminise kvantifikatore u svakoj $\mathcal{L}$ -formuli $\varphi(\bar{v})$.

Teorema. ACF eliminise kvantifikatore.

Dokaz NH_3

Neka je $I = \langle f_1, \dots, f_m \rangle \neq \emptyset$, neka je $M \supseteq I$ maksimalan nadideal, neka je $E = F[\overline{X}]/M$ količničko polje, i neka je $\overline{E}$ algebarsko zatvorenje od E .

Tada $\overline{E} \models \exists \bar{x} \varphi(\bar{x}, \bar{a})$, gde su $\bar{a} \in F$ koeficijenti polinoma $f_1, \dots, f_m$ i $\varphi(\bar{x}, \bar{a})$ je konjunkcija formula $f_i(\bar{x}) = 0$.

Prema QE, $ACF \models (\forall \bar{v})(\exists \bar{x} \varphi(\bar{x}, \bar{v}) \leftrightarrow \psi(\bar{v}))$ gde je $\psi(\bar{v})$ beskvantorna, pa $\overline{E} \models \psi(\bar{a})$.

Kako je $F \leq \overline{E}$, $\bar{a} \in F$ i $\psi(\bar{v})$ je beskvantorna, $F \models \psi(\bar{a})$.

Kako $F \models ACF$, $F \models \exists \bar{x} \varphi(\bar{x}, \bar{a})$.

Teorema. Neka je T $\mathcal{L}$ -teorija. Sledeći iskazi su ekvivalentni:

- (1) T eliminiše kvantifikatore;
- (2) za svaku beskvantornu $\mathcal{L}$ -formulu $\varphi(x, \bar{v})$, T eliminiše kvantifikator u $\exists x \varphi(x, \bar{v})$.

Komentar. U prethodnoj teoremi možemo da pretpostavimo da je $\varphi(x, \bar{v})$ konjunkcija literala (atomske i negacije atomskih formula) u kojima se x pojavljuje.

Definicija. Formula je *prosta* ako je oblika $\exists x \varphi(x, \bar{v})$, gde je $\varphi(x, \bar{v})$ konjunkcija literala u kojima se x pojavljuje.

Teorema. *DLO* eliminiše kvantifikatore.

Semantički kriterijum za QE

Definicija. Za $\mathcal{L}$ -strukture $\mathcal{A}$ i $\mathcal{B}$, $n \in \mathbb{N}$, $\bar{a} \in A^n$ i $\bar{b} \in B^n$, pišemo $(\mathcal{A}, \bar{a}) \equiv (\mathcal{B}, \bar{b})$ ako za sve $\mathcal{L}$ -formule $\varphi(\bar{v})$ važi:

$$\mathcal{A} \models \varphi(\bar{a}) \iff \mathcal{B} \models \varphi(\bar{b}).$$

Pišemo $(\mathcal{A}, \bar{a}) \equiv_s (\mathcal{B}, \bar{b})$ ako prethodna ekvivalencija važi za sve proste $\mathcal{L}$ -formule $\varphi(\bar{v})$.

Teorema. Neka je T $\mathcal{L}$ -teorija. Sledeći iskazi su ekvivalentni:

(1) T eliminiše kvantifikatore;

(2) $(\forall \mathcal{A}, \mathcal{B} \models T)(\forall n \in \mathbb{N})(\forall \bar{a} \in A^n, \bar{b} \in B^n)$

$$(\mathcal{A}, \bar{a}) \equiv_{qf} (\mathcal{B}, \bar{b}) \Rightarrow (\mathcal{A}, \bar{a}) \equiv (\mathcal{B}, \bar{b});$$

(3) $(\forall \mathcal{A}, \mathcal{B} \models T)(\forall n \in \mathbb{N})(\forall \bar{a} \in A^n, \bar{b} \in B^n)$

$$(\mathcal{A}, \bar{a}) \equiv_{qf} (\mathcal{B}, \bar{b}) \Rightarrow (\mathcal{A}, \bar{a}) \equiv_s (\mathcal{B}, \bar{b}).$$

Teorema. *ACF* eliminiše kvantifikatore.