Teoria de Modelos e Aplicações

Caio Lopes, Henrique Lecco

ICMC - USP

30 de julho de 2020

Objetivos

Os objetivos da aula de hoje são:

Objetivos

Os objetivos da aula de hoje são:

- Definir eliminação de quantificadores e provar uma caracterização

Objetivos

Os objetivos da aula de hoje são:

- Definir eliminação de quantificadores e provar uma caracterização
- Definir *RCF* e provar que essa teoria elimina quantificadores;

Objetivos

Os objetivos da aula de hoje são:

- Definir eliminação de quantificadores e provar uma caracterização
- Definir *RCF* e provar que essa teoria elimina quantificadores;
- Enunciar e demonstrar o 17° problema de Hilbert.

Objetivos

Os objetivos da aula de hoje são:

- Definir eliminação de quantificadores e provar uma caracterização
- Definir *RCF* e provar que essa teoria elimina quantificadores;
- Enunciar e demonstrar o 17° problema de Hilbert.

Observação: As referências para as demonstrações dos fatos algébrico que iremos assumir podem ser encontradas na bibliografia do curso, que está listada no github. Também recomendamos o livro Model Theory of Fields, do David Marker.

Revisão

Definições:

1. Uma teoria T é consistente se não existe uma fórmula ϕ tal que $T \models \phi$ e $T \models \neg\phi$;

Revisão

Definições:

1. Uma teoria T é consistente se não existe uma fórmula ϕ tal que $T \models \phi$ e $T \models \neg\phi$;
2. Uma fórmula é atômica se é do tipo $t_1 = t_2$ ou $\mathbf{r}(t_1, ..., t_n)$;

Revisão

Resultados

1. Se uma teoria é consistente, então ela admite um modelo;

Revisão

Resultados

1. Se uma teoria é consistente, então ela admite um modelo;
2. **Compacidade** Uma teoria admite modelo se, e somente se, todas as suas coleções finitas de sentenças admitem modelo.

Eliminação de quantificadores

Definição: Uma teoria T admite eliminação de quantificadores se para toda fórmula $\phi(v, x_1, ..., x_m)$, existe uma fórmula $\psi(v, x_1, ..., x_m)$ livre de quantificadores de forma que

$$T \models \forall v[\phi(v, x_1, ..., x_m) \leftrightarrow \psi(v, x_1, ..., x_m)]$$

Teorema de caracterização

Teorema(Teste do João): Seja L uma linguagem contendo ao menos um símbolo de constante. Sejam T uma L-teoria e $\phi(x_1, ..., x_m)$ uma L-fórmula. São equivalentes:

Teorema de caracterização

Teorema(Teste do João): Seja L uma linguagem contendo ao menos um símbolo de constante. Sejam T uma L-teoria e $\phi(x_1, ..., x_m)$ uma L-fórmula. São equivalentes:

1. Existe uma fórmula $\psi(x_1, ..., x_m)$ livre de quantificadores tal que $T \models \forall \overline{x}(\phi(\overline{x}) \leftrightarrow \psi(\overline{x}))$

Teorema de caracterização

Teorema(Teste do João): Seja L uma linguagem contendo ao menos um símbolo de constante. Sejam T uma L-teoria e $\phi(x_1, ..., x_m)$ uma L-fórmula. São equivalentes:

1. Existe uma fórmula $\psi(x_1, ..., x_m)$ livre de quantificadores tal que $T \models \forall \overline{x}(\phi(\overline{x}) \leftrightarrow \psi(\overline{x}))$
2. Se M e N são modelos tais que $M, N \models T$ e C é um modelo de forma que $C \subset M$ e $C \subset N$, então $M \models \phi(\overline{a})$ se, e somente se, $N \models \phi(\overline{a})$ para todo $\overline{a} \in C$

Prova:

Prova:

$1) \Rightarrow 2)$:

Prova:

1) $\Rightarrow$ 2) : Seja $\overline{a} \in C$. Temos que:

Prova:

1) $\Rightarrow$ 2) : Seja $\overline{a} \in C$. Temos que:

$M \models \phi(\overline{a})$

Prova:

1) $\Rightarrow$ 2) : Seja $\overline{a} \in C$. Temos que:

$M \models \phi(\overline{a})$

$\Leftrightarrow M \models \psi(\overline{a})$ pois $M \models \forall \overline{v}(\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$

Prova:

1) $\Rightarrow$ 2) : Seja $\overline{a} \in C$. Temos que:

$M \models \phi(\overline{a})$

$\Leftrightarrow M \models \psi(\overline{a})$ pois $M \models \forall \overline{v}(\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$
$\Leftrightarrow C \models \psi(\overline{a})$ pois $C \subset M$ e $\psi(\overline{x})$ é livre de quantificadores

Prova:

1) $\Rightarrow$ 2) : Seja $\overline{a} \in C$. Temos que:

$M \models \phi(\overline{a})$

$\Leftrightarrow M \models \psi(\overline{a})$ pois $M \models \forall \overline{v}(\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$
$\Leftrightarrow C \models \psi(\overline{a})$ pois $C \subset M$ e $\psi(\overline{x})$ é livre de quantificadores
$\Leftrightarrow N \models \psi(\overline{a})$ pois $C \subset N$ e $\psi(\overline{x})$ é livre de quantificadores

Prova:

1) $\Rightarrow$ 2) : Seja $\overline{a} \in C$. Temos que:

$M \models \phi(\overline{a})$

$\Leftrightarrow M \models \psi(\overline{a})$ pois $M \models \forall \overline{v}(\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$
$\Leftrightarrow C \models \psi(\overline{a})$ pois $C \subset M$ e $\psi(\overline{x})$ é livre de quantificadores
$\Leftrightarrow N \models \psi(\overline{a})$ pois $C \subset N$ e $\psi(\overline{x})$ é livre de quantificadores

$2) \Rightarrow 1)$:

$2) \Rightarrow 1)$:

Seja $\phi(\overline{x})$ uma $L-$fórmula. Primeiro, suponha que $\phi(\overline{x})$ não é consistente com T. Então $T \models \forall \overline{v} \neg \phi(\overline{x})$, então se c é um símbolo de constante da linguagem, segue que $T \models \forall \overline{v}[\phi(\overline{v}) \leftrightarrow c \neq c]$. Ou seja, ϕ é equivalente a uma fórmula sem quantificadores $(c \neq c)$.

$2) \Rightarrow 1)$:

Seja $\phi(\overline{x})$ uma $L-$fórmula. Primeiro, suponha que $\phi(\overline{x})$ não é consistente com T. Então $T \models \forall \overline{v} \neg \phi(\overline{x})$, então se c é um símbolo de constante da linguagem, segue que $T \models \forall \overline{v}[\phi(\overline{v}) \leftrightarrow c \neq c]$. Ou seja, ϕ é equivalente a uma fórmula sem quantificadores $(c \neq c)$. Analogamente, se $\neg\phi(\overline{x})$ não é consistente com T, temos que $T \models \forall \overline{v}[\phi(\overline{v}) \leftrightarrow c = c]$.

$2) \Rightarrow 1)$:

Seja $\phi(\overline{x})$ uma $L-$fórmula. Primeiro, suponha que $\phi(\overline{x})$ não é consistente com T. Então $T \models \forall \overline{v} \neg \phi(\overline{x})$, então se c é um símbolo de constante da linguagem, segue que $T \models \forall \overline{v}[\phi(\overline{v}) \leftrightarrow c \neq c]$. Ou seja, ϕ é equivalente a uma fórmula sem quantificadores $(c \neq c)$. Analogamente, se $\neg\phi(\overline{x})$ não é consistente com T, temos que $T \models \forall \overline{v}[\phi(\overline{v}) \leftrightarrow c = c]$.

Assim, vamos nos concentrar nos casos em que $\phi(\overline{x})$ e $\neg\phi(\overline{x})$ são consistentes com T.

Defina

$\Gamma := \{\psi(\overline{x}) : \psi(\overline{x})$ é livre de quantificadores e $T \vdash \forall \overline{x}(\phi(\overline{x}) \to \psi(\overline{x}))\}$,

isto é, o conjunto de fórmulas livres de quantificadores que são consequência de $\phi(\overline{x})$.

Afirmação: $T \cup \Gamma(\overline{d}) \vdash \phi(\overline{d})$

Afirmação: $T \cup \Gamma(\overline{d}) \vdash \phi(\overline{d})$

Prova: Suponha que não. Então $T \cup \Gamma(\overline{d}) \cup \{\neg\phi(\overline{d})\}$ é consistente pois $T \cup \Gamma(\overline{d})$ é consistente e estamos assumindo $\neg\phi$ consistente. Portanto existe um modelo M tal que

$$M \models T \cup \Gamma(\overline{d}) \cup \{\neg\phi(\overline{d})\}.$$

Afirmação: $T \cup \Gamma(\overline{d}) \vdash \phi(\overline{d})$

Prova: Suponha que não. Então $T \cup \Gamma(\overline{d}) \cup \{\neg\phi(\overline{d})\}$ é consistente pois $T \cup \Gamma(\overline{d})$ é consistente e estamos assumindo $\neg\phi$ consistente. Portanto existe um modelo M tal que

$$M \models T \cup \Gamma(\overline{d}) \cup \{\neg\phi(\overline{d})\}.$$

Seja C o submodelo de M gerado por $\overline{d}$, isto é, o menor submodelo de M que contém $\overline{d}$ em seu universo, é fechado pelas funções da linguagem e contém as constantes da linguagem, ou ainda, C é o conjunto de termos da linguagem com parâmetros $\overline{d}$.

Afirmação: $T \cup \Gamma(\overline{d}) \vdash \phi(\overline{d})$

Prova: Suponha que não. Então $T \cup \Gamma(\overline{d}) \cup \{\neg\phi(\overline{d})\}$ é consistente pois $T \cup \Gamma(\overline{d})$ é consistente e estamos assumindo $\neg\phi$ consistente. Portanto existe um modelo M tal que

$$M \models T \cup \Gamma(\overline{d}) \cup \{\neg\phi(\overline{d})\}.$$

Seja C o submodelo de M gerado por $\overline{d}$, isto é, o menor submodelo de M que contém $\overline{d}$ em seu universo, é fechado pelas funções da linguagem e contém as constantes da linguagem, ou ainda, C é o conjunto de termos da linguagem com parâmetros $\overline{d}$.

Como $C \subset M$, $M \models \Gamma(\overline{d})$ e todas as fórmulas de $\Gamma(\overline{d})$ são livres de quantificadores, então $C \models \Gamma(\overline{d})$.

Defina $L_{\overline{d}}$ a linguagem L acrescentada de uma constante para cada entrada de $\overline{d}$.

Defina $L_{\overline{d}}$ a linguagem L acrescentada de uma constante para cada entrada de $\overline{d}$.

Agora tome $Diag(C)$ o conjunto das fórmulas atômicas ou negação de atômicas (com parâmetros em C) que são verdade em C com a linguagem $L_{\overline{d}}$.

Defina $L_{\overline{d}}$ a linguagem L acrescentada de uma constante para cada entrada de $\overline{d}$.

Agora tome $Diag(C)$ o conjunto das fórmulas atômicas ou negação de atômicas (com parâmetros em C) que são verdade em C com a linguagem $L_{\overline{d}}$.

Seja $\Sigma = T \cup Diag(C) \cup \{\phi(\overline{d})\}$.

Afirmação: Σ é consistente.

Afirmação: Σ é consistente.

Prova: Suponha que Σ não é consistente. Então $T \cup Diag(C) \models \neg\phi(\overline{d})$ pois admite modelo.

Afirmação: Σ é consistente.

Prova: Suponha que Σ não é consistente. Então $T \cup Diag(C) \models \neg\phi(\overline{d})$ pois admite modelo.

Por compacidade, existem $\psi_1(\overline{d}), ..., \psi_n(\overline{d}) \in Diag(C)$ tais que

$$T \models \forall \overline{v} \left(\left(\bigwedge_{i=1}^{n} \psi_i(\overline{v}) \right) \rightarrow \neg\phi(\overline{v}) \right),$$

Afirmação: Σ é consistente.

Prova: Suponha que Σ não é consistente. Então $T \cup Diag(C) \models \neg\phi(\overline{d})$ pois admite modelo.

Por compacidade, existem $\psi_1(\overline{d}), ..., \psi_n(\overline{d}) \in Diag(C)$ tais que

$$T \models \forall \overline{v} \left(\left(\bigwedge_{i=1}^{n} \psi_i(\overline{v}) \right) \rightarrow \neg\phi(\overline{v})) \right),$$

que é equivalente a

$$T \models \forall \overline{v} \left(\phi(\overline{v}) \rightarrow \left(\bigvee_{i=1}^{n} \neg\psi_i(\overline{v}) \right) \right)$$

Para cada $1 \leq i \leq n$, $\psi_i(\overline{v})$ é atômica ou negação de atômica, o que significa que $\psi_i(\overline{v})$ é livre de quantificadores, então $\bigvee_{i=1}^{n} \neg\psi_i(\overline{v}) \in \Gamma$.

Para cada $1 \leq i \leq n$, $\psi_i(\overline{v})$ é atômica ou negação de atômica, o que significa que $\psi_i(\overline{v})$ é livre de quantificadores, então $\bigvee_{i=1}^{n} \neg\psi_i(\overline{v}) \in \Gamma$.

Portanto, $C \models \bigvee_{i=1}^{n} \neg\psi_i(\overline{d})$ (pois $C \models \Gamma(\overline{d})$), logo, para ao menos um $1 \leq i \leq n$, temos que $C \models \neg\psi_i(\overline{d})$, mas $\psi_i(\overline{d}) \in Diag(C)$, portanto $C \models \psi_i(\overline{d})$, contradição.

Voltemos a demonstração da afirmação. Temos que Σ é consistente. Seja N um modelo tal que $N \models \Sigma$. Como $\phi(\overline{d}) \in \Sigma$, segue que $N \models \phi(\overline{d})$. Como $Diag(C) \subset \Sigma$, toda fórmula livre de quantificadores com parâmetros em C e que é verdade em C é verdade em N, portanto $C \subset N$.

Voltemos a demonstração da afirmação. Temos que Σ é consistente. Seja N um modelo tal que $N \models \Sigma$. Como $\phi(\overline{d}) \in \Sigma$, segue que $N \models \phi(\overline{d})$. Como $Diag(C) \subset \Sigma$, toda fórmula livre de quantificadores com parâmetros em C e que é verdade em C é verdade em N, portanto $C \subset N$.

Temos, por hipótese, que se $M \models \neg\phi(\overline{d})$, $\overline{d} \in C$, $C \subset M$ e $C \subset N$, então $N \models \neg\phi(\overline{d})$, absurdo pois $N \models \phi(\overline{d})$ e é consistente.

Voltemos a demonstração da afirmação. Temos que Σ é consistente. Seja N um modelo tal que $N \models \Sigma$. Como $\phi(\overline{d}) \in \Sigma$, segue que $N \models \phi(\overline{d})$. Como $Diag(C) \subset \Sigma$, toda fórmula livre de quantificadores com parâmetros em C e que é verdade em C é verdade em N, portanto $C \subset N$.

Temos, por hipótese, que se $M \models \neg\phi(\overline{d})$, $\overline{d} \in C$, $C \subset M$ e $C \subset N$, então $N \models \neg\phi(\overline{d})$, absurdo pois $N \models \phi(\overline{d})$ e é consistente.

Isso conclui a demonstração da afirmação. Voltemos a demonstração do Teorema.

Então temos que $T \cup \Gamma(\overline{d}) \models \phi(\overline{d})$. Por compacidade, existem $\psi_1, ..., \psi_n \in \Gamma$ de forma que $T \models \forall \overline{v}(\bigwedge_{i=1}^{n} \psi_i(\overline{v}) \rightarrow \phi(\overline{v}))$.

Então temos que $T \cup \Gamma(\overline{d}) \models \phi(\overline{d})$. Por compacidade, existem $\psi_1, ..., \psi_n \in \Gamma$ de forma que $T \models \forall \overline{v}(\bigwedge_{i=1}^{n} \psi_i(\overline{v}) \rightarrow \phi(\overline{v}))$.

Logo, $T \models \forall \overline{v}(\bigwedge_{i=1}^{n} \psi_i(\overline{v}) \leftrightarrow \phi(\overline{v}))$ e $\bigwedge_{i=1}^{n} \psi_i(\overline{v})$ é livre de quantificadores. $\square$

Corpos Reais Fechados

O conceito de corpo real fechado é a generalização dos números reais.

Corpos Reais Fechados

O conceito de corpo real fechado é a generalização dos números reais.

Definição:

Corpos Reais Fechados

O conceito de corpo real fechado é a generalização dos números reais.

Definição:

1. Um corpo F é formalmente real se -1 *não é* a soma de quadrados.

Corpos Reais Fechados

O conceito de corpo real fechado é a generalização dos números reais.

Definição:

1. Um corpo F é formalmente real se -1 *não é* a soma de quadrados.
2. Um corpo é real fechado se é formalmente real e não pode ser estendido por um corpo formalmente real.

Corpos Reais Fechados

A teoria de corpos reais fechados é denotada por RCF (Real Closed Fields).

Corpos Reais Fechados

A teoria de corpos reais fechados é denotada por RCF (Real Closed Fields).

Voltemos, mais uma vez, à linguagem de anéis $L_{ring} = \{0, 1, +, \cdot\}$. Mas dessa vez, iremos adicionar um símbolo de relação que representará uma ordem: $L_{oring} = L_{ring} \cup \{<\}$.

Teorema de Artin-Schreier

Teorema: Seja F um corpo formalmente real. São equivalentes:

Teorema de Artin-Schreier

Teorema: Seja F um corpo formalmente real. São equivalentes:

1. F é fechado real;

Teorema de Artin-Schreier

Teorema: Seja F um corpo formalmente real. São equivalentes:

1. F é fechado real;
2. Para todo $a \in F$, existe b tal que $b^2 = a$ ou $b^2 = -a$. Além disso, todo polinômio de grau ímpar tem raiz.

RCF

A definição da teoria *RCF* é corolário do teorema anterior. Ela é dada por:

- Axiomas de corpo;

RCF

A definição da teoria *RCF* é corolário do teorema anterior. Ela é dada por:

- Axiomas de corpo;
- Sentenças garantindo que -1 não é a soma de quadrados, isto é, para cada $n \in \mathbb{N}$

$$(\forall x_1, ..., x_n) x_1^2 + ... + x_n^2 + 1 \neq 0$$

RCF

A definição da teoria *RCF* é corolário do teorema anterior. Ela é dada por:

- Axiomas de corpo;
- Sentenças garantindo que -1 não é a soma de quadrados, isto é, para cada $n \in \mathbb{N}$

$$(\forall x_1, ..., x_n) x_1^2 + ... + x_n^2 + 1 \neq 0$$

- Uma sentença garantindo que todo elemento ou seu negativo é um quadrado, isto é,

$$(\forall x \exists y)[y^2 = x] \vee [y^2 + x = 0]$$

RCF

A definição da teoria *RCF* é corolário do teorema anterior. Ela é dada por:

- Axiomas de corpo;
- Sentenças garantindo que -1 não é a soma de quadrados, isto é, para cada $n \in \mathbb{N}$

$$(\forall x_1, ..., x_n) x_1^2 + ... + x_n^2 + 1 \neq 0$$

- Uma sentença garantindo que todo elemento ou seu negativo é um quadrado, isto é,

$$(\forall x \exists y)[y^2 = x] \vee [y^2 + x = 0]$$

- Sentenças garantindo que todo polinômio de grau ímpar tem raiz, isto é, para cada $n \in \mathbb{N}$

$$(\forall x_0, ..., x_{2n+1} \exists y) x_{2n+1} y^{2n+1} + ... + x1y + x_0 = 0$$

RCF

A definição da teoria *RCF* é corolário do teorema anterior. Ela é dada por:

- Axiomas de corpo;
- Sentenças garantindo que -1 não é a soma de quadrados, isto é, para cada $n \in \mathbb{N}$

$$(\forall x_1, ..., x_n) x_1^2 + ... + x_n^2 + 1 \neq 0$$

- Uma sentença garantindo que todo elemento ou seu negativo é um quadrado, isto é,

$$(\forall x \exists y)[y^2 = x] \vee [y^2 + x = 0]$$

- Sentenças garantindo que todo polinômio de grau ímpar tem raiz, isto é, para cada $n \in \mathbb{N}$

$$(\forall x_0, ..., x_{2n+1} \exists y) x_{2n+1} y^{2n+1} + ... + x1y + x_0 = 0$$

RCF

Temos o necessário para provar que *RCF* elimina quantificadores.

RCF

Temos o necessário para provar que *RCF* elimina quantificadores.

Teorema: *RCF* admite eliminação de quantificadores.

RCF

Temos o necessário para provar que *RCF* elimina quantificadores.

Teorema: *RCF* admite eliminação de quantificadores.

Prova:

RCF

Temos o necessário para provar que RCF elimina quantificadores.

Teorema: RCF admite eliminação de quantificadores.

Prova:

Sejam F_1, F_2 modelos de RCF e $K \subset F_1, F_2$. Seja K' o corpo de frações de K.

RCF

Temos o necessário para provar que RCF elimina quantificadores.

Teorema: RCF admite eliminação de quantificadores.

Prova:

Sejam F_1, F_2 modelos de RCF e $K \subset F_1, F_2$. Seja K' o corpo de frações de K.

Precisaremos de outro teorema, também provado por Artin e Schreier: Todo corpo ordenado tem um único fecho algébrico real (a menos de isomorfismo).

Seja R o fecho algébrico de K', que é único e portanto $R \subset F_1, F_2$.
Sejam $\phi(v, \overline{w})$ uma fórmula livre de quantificadores, $\overline{a} \in K$ e $b \in F_1$.

Seja R o fecho algébrico de K', que é único e portanto $R \subset F_1, F_2$. Sejam $\phi(v, \overline{w})$ uma fórmula livre de quantificadores, $\overline{a} \in K$ e $b \in F_1$.

Suponha que $F_1 \models \phi(b, \overline{a})$, ou seja, $F_1 \models \exists v \phi(v, \overline{a})$. Queremos mostrar que $F_2 \models \exists v \phi(v, \overline{a})$. Note que é suficiente mostrarmos que $R \models \exists v \phi(v, \overline{a})$.

Como ϕ é livre de quantificadores, existem polinômios $f_1, ..., f_n, g_1, ..., g_m \in K[x]$ tal que $\phi(v, \overline{a})$ é equivalente a

$$\left(\bigwedge_{i=1}^{n} f_i(v) = 0 \right) \wedge \left(\bigwedge_{i=1}^{m} g_i(v) > 0 \right)$$

Como ϕ é livre de quantificadores, existem polinômios $f_1, ..., f_n, g_1, ..., g_m \in K[x]$ tal que $\phi(v, \overline{a})$ é equivalente a

$$\left(\bigwedge_{i=1}^{n} f_i(v) = 0 \right) \wedge \left(\bigwedge_{i=1}^{m} g_i(v) > 0 \right)$$

Como $F_1 \models \phi(b, \overline{a})$, segue que $f_i(b) = 0$ para algum i. Ou seja, b é algébrico sobre K e portanto $b \in R \subset F_2$, que é fecho algébrico. Portanto só precisamos considerar $\phi(v, \overline{a})$ da forma

$$\bigwedge_{i=1}^{n} g_i(v) > 0$$

Outro resultado algébrico nos diz que: se F é corpo real fechado e $f \in F[x]$, então f pode ser reescrito em fatores do tipo $(x - a)$ ou $(x - a)^2 + b^2$ para alguns $a, b \in F, b \neq 0$.

Outro resultado algébrico nos diz que: se F é corpo real fechado e $f \in F[x]$, então f pode ser reescrito em fatores do tipo $(x - a)$ ou $(x - a)^2 + b^2$ para alguns $a, b \in F, b \neq 0$.

Fatore cada g_i como descrito acima. Note que como $(x - a)^2 + b^2 \geq 0$ para todos a, b, x, segue que para que $g_i > 0$ é necessário apenas que um número par dos termos $(x - c_{1_i})...(x - c_{p_i})$ seja negativo.

Sem perda de generalidade, suponha que $c_{j_i} \leq c_{k_i}$ para $1 \leq j < k \leq p_i$.

Sem perda de generalidade, suponha que $c_{j_i} \leq c_{k_i}$ para $1 \leq j < k \leq p_i$.

Afirmação: $g_i(x) > 0$ se e somente se:

- Caso p_i for ímpar:

$$\bigvee_{j=1}^{\frac{p_i-1}{2}} [c_{(2j-1)_i} < x \wedge x < c_{(2j)_i}] \vee c_{p_i} < x$$

- Caso p_i for par:

$$x < c_{1_i} \vee \bigvee_{j=1}^{\frac{p_i-2}{2}} [c_{(2j)_i} < x \wedge x < c_{(2j+1)_i}] \vee c_{p_i} < x$$

Sem perda de generalidade, suponha que $c_{j_i} \leq c_{k_i}$ para $1 \leq j < k \leq p_i$.

Afirmação: $g_i(x) > 0$ se e somente se:

- Caso p_i for ímpar:

$$\bigvee_{j=1}^{\frac{p_i-1}{2}} [c_{(2j-1)_i} < x \wedge x < c_{(2j)_i}] \vee c_{p_i} < x$$

- Caso p_i for par:

$$x < c_{1_i} \vee \bigvee_{j=1}^{\frac{p_i-2}{2}} [c_{(2j)_i} < x \wedge x < c_{(2j+1)_i}] \vee c_{p_i} < x$$

Exercício

Sem perda de generalidade, suponha que $c_{j_i} \leq c_{k_i}$ para $1 \leq j < k \leq p_i$.

Afirmação: $g_i(x) > 0$ se e somente se:

- Caso p_i for ímpar:

$$\bigvee_{j=1}^{\frac{p_i-1}{2}} [c_{(2j-1)_i} < x \wedge x < c_{(2j)_i}] \vee c_{p_i} < x$$

- Caso p_i for par:

$$x < c_{1_i} \vee \bigvee_{j=1}^{\frac{p_i-2}{2}} [c_{(2j)_i} < x \wedge x < c_{(2j+1)_i}] \vee c_{p_i} < x$$

Exercício :p

Seja $\theta(x, c_{1_1}, ..., c_{p_m})$ a conjunção de todas as fórmulas anteriores. Note que essa fórmula é equivalente a

$$\bigwedge_{i=1}^{n} f_i(v) = 0 \wedge \bigwedge_{i=1}^{m} g_i(v) > 0,$$

que por sua vez já vimos ser equivalente a $\phi(v, \overline{a})$

Seja $c_{max} = max\{c_{p_i} : 1 \leq i \leq m\} \geq 1$. Note que $c_{max} \in R$, pois cada $c_{p_i} \in R$, por hipótese. Portanto $c_{max} \in F_2$. Note também que, como $c_{max} \leq c_{p_i}$ para todo i, temos que $R \models \theta(c_{max}, c_{1_1}, ..., c_{p_m})$.

Seja $c_{max} = max\{c_{p_i} : 1 \leq i \leq m\} \geq 1$. Note que $c_{max} \in R$, pois cada $c_{p_i} \in R$, por hipótese. Portanto $c_{max} \in F_2$. Note também que, como $c_{max} \leq c_{p_i}$ para todo i, temos que $R \models \theta(c_{max}, c_{1_1}, ..., c_{p_m})$.

Portanto $R \models \phi(c_{max}, \bar{a})$ que é equivalente a $R \models \exists v\ \phi(v, \bar{a})$. Como $R \subset F_2$, segue que $F_2 \models \exists v\ \phi(v, \bar{a})$.

Seja $c_{max} = max\{c_{p_i} : 1 \leq i \leq m\} \geq 1$. Note que $c_{max} \in R$, pois cada $c_{p_i} \in R$, por hipótese. Portanto $c_{max} \in F_2$. Note também que, como $c_{max} \leq c_{p_i}$ para todo i, temos que $R \models \theta(c_{max}, c_{1_1}, ..., c_{p_m})$.

Portanto $R \models \phi(c_{max}, \bar{a})$ que é equivalente a $R \models \exists v\ \phi(v, \bar{a})$. Como $R \subset F_2$, segue que $F_2 \models \exists v\ \phi(v, \bar{a})$.

Aplicando o Teste de João, existe uma fórmula livre de quantificadores equivalente a ϕ, como queríamos. $\square$

Proposição: Eliminação de quantificadores $\Rightarrow$ modelo-completo.

Proposição: Eliminação de quantificadores $\Rightarrow$ modelo-completo.

Corolário: RCF é modelo-completo.

17° problema de Hilbert

Definição: Seja F um corpo real fechado e $f \in F(\overline{x})$ uma função racional em n variáveis ($f(\overline{x}) = \frac{p(\overline{x})}{q(\overline{x})}$). Dizemos que f é positiva semidefinida se $f(\overline{a}) \geq 0$ para todo $\overline{a} \in F^n$.

17° problema de Hilbert

A motivação de Hilbert incluir esse problema na sua lista veio de um outro problema que ele resolveu. Ele mostrou que existem polinômios positivos semidefinidos que não podem ser escritos como a soma de quadrados de polinômios. Por exemplo:

17° problema de Hilbert

A motivação de Hilbert incluir esse problema na sua lista veio de um outro problema que ele resolveu. Ele mostrou que existem polinômios positivos semidefinidos que não podem ser escritos como a soma de quadrados de polinômios. Por exemplo:

$$M(x, y) = x^4y^2 + x^2y^4 + 1 - 3x^2y^2$$

17° problema de Hilbert

A motivação de Hilbert incluir esse problema na sua lista veio de um outro problema que ele resolveu. Ele mostrou que existem polinômios positivos semidefinidos que não podem ser escritos como a soma de quadrados de polinômios. Por exemplo:

$$M(x, y) = x^4y^2 + x^2y^4 + 1 - 3x^2y^2$$

Entretanto, é possível escrever esse polinômio como a soma de quadrados de funções racionais:

17° problema de Hilbert

A motivação de Hilbert incluir esse problema na sua lista veio de um outro problema que ele resolveu. Ele mostrou que existem polinômios positivos semidefinidos que não podem ser escritos como a soma de quadrados de polinômios. Por exemplo:

$$M(x,y) = x^4y^2 + x^2y^4 + 1 - 3x^2y^2$$

Entretanto, é possível escrever esse polinômio como a soma de quadrados de funções racionais:

$$M(x,y) = \frac{x^2y^2(x^2+y^2+1)(x^2+y^2-2) + (x^2-y^2)^2}{(x^2+y^2)^2}$$

17° problema de Hilbert

Um último Teorema de Artin-Schreier antes de provarmos o teorema.
Teorema: Se F é formalmente real e se $a \in F$ não é a soma de quadrados, então existe uma ordem em F tal que a é negativo.

17° problema de Hilbert

Um último Teorema de Artin-Schreier antes de provarmos o teorema.
Teorema: Se F é formalmente real e se $a \in F$ não é a soma de quadrados, então existe uma ordem em F tal que a é negativo.

Teorema: Se $f \in F(\overline{x})$ é uma função racional positiva semidefinida sobre um corpo real fechado F, então f é a soma de quadrados de funções racionais.

Prova: Seja $f(x_1, ..., x_n)$ uma função racional positiva semidefinida que não é a soma de quadrados de funções racionais.

Prova: Seja $f(x_1, ..., x_n)$ uma função racional positiva semidefinida que não é a soma de quadrados de funções racionais.

Por um dos teoremas antei que vimos, existe uma ordem $\leq$ de $F(\overline{x})$ de forma que $f < 0$. Seja R uma extensão fechada, real e que estende $\leq$.

Prova: Seja $f(x_1, ..., x_n)$ uma função racional positiva semidefinida que não é a soma de quadrados de funções racionais.

Por um dos teoremas antei que vimos, existe uma ordem $\leq$ de $F(\overline{x})$ de forma que $f < 0$. Seja R uma extensão fechada, real e que estende $\leq$.

Note que

$$R \models (\exists \overline{v}) f(\overline{v}) < 0$$

Prova: Seja $f(x_1, ..., x_n)$ uma função racional positiva semidefinida que não é a soma de quadrados de funções racionais.

Por um dos teoremas antei que vimos, existe uma ordem $\leq$ de $F(\overline{x})$ de forma que $f < 0$. Seja R uma extensão fechada, real e que estende $\leq$.

Note que

$$R \models (\exists \overline{v}) f(\overline{v}) < 0$$

Como RCF é modelo-completa e $F \subset R$, segue que

Prova: Seja $f(x_1, ..., x_n)$ uma função racional positiva semidefinida que não é a soma de quadrados de funções racionais.

Por um dos teoremas antei que vimos, existe uma ordem $\leq$ de $F(\overline{x})$ de forma que $f < 0$. Seja R uma extensão fechada, real e que estende $\leq$.

Note que

$$R \models (\exists \overline{v}) f(\overline{v}) < 0$$

Como RCF é modelo-completa e $F \subset R$, segue que

$$F \models (\exists \overline{v}) f(\overline{v}) < 0$$

Prova: Seja $f(x_1, ..., x_n)$ uma função racional positiva semidefinida que não é a soma de quadrados de funções racionais.

Por um dos teoremas antei que vimos, existe uma ordem $\leq$ de $F(\overline{x})$ de forma que $f < 0$. Seja R uma extensão fechada, real e que estende $\leq$.

Note que

$$R \models (\exists \overline{v}) f(\overline{v}) < 0$$

Como RCF é modelo-completa e $F \subset R$, segue que

$$F \models (\exists \overline{v}) f(\overline{v}) < 0$$

Ou seja, existe $\overline{a} \in F^n$ tal que $f(\overline{a}) < 0$, absurdo pois f é positiva semidefinida. $\square$

Acabou

Até segunda! :)