Modelos e Aplicações - Aula 11

Caio Lopes, Henrique Lecco

ICMC - USP

5 de agosto de 2020

Ultraprodutos

Dado um conjunto I e, para cada $i \in I$ um modelo $\mathcal{M}_i$, seja $\mathfrak{U}$ um ultrafiltro sobre I.
Definimos $\mathcal{M}^*$ como sendo o ultraproduto dos $\mathcal{M}_i$ sobre o ultrafiltro $\mathfrak{U}$. Não vamos fazer a construção inteira de novo.

Ultraprodutos

Dado um conjunto I e, para cada $i \in I$ um modelo $\mathcal{M}_i$, seja $\mathfrak{U}$ um ultrafiltro sobre I.
Definimos $\mathcal{M}^*$ como sendo o ultraproduto dos $\mathcal{M}_i$ sobre o ultrafiltro $\mathfrak{U}$. Não vamos fazer a construção inteira de novo.

Os elementos de M^* são classes de equivalência de "sequências" $\langle x_i \rangle_{i \in I}$ pela relação $=_{\mathfrak{U}}$, que define que o conjunto de coordenadas em que as sequências coincidem está contido no ultrafiltro.

Na maior parte do tempo, dependemos simplesmente da caracterização garantida pelo Teorema de Łoś:

Teorema

$\mathcal{M}^* \models \varphi(a) \Leftrightarrow \{i \in I : \mathcal{M}_i \models \varphi(a_i)\} \in \mathfrak{U}.$

Análise não standard

Seja $\mathfrak{U}$ um ultrafiltro sobre $\mathbb{N}$ que não contém subconjuntos finitos. e considere, na linguagem de anéis ordenados:

$$\mathcal{M}^* = \frac{\prod_{i\in\mathbb{N}} \mathbb{R}}{\mathfrak{U}}$$

Análise não standard

Seja $\mathfrak{U}$ um ultrafiltro sobre $\mathbb{N}$ que não contém subconjuntos finitos. e considere, na linguagem de anéis ordenados:

$$\mathcal{M}^* = \frac{\prod_{i\in\mathbb{N}} \mathbb{R}}{\mathfrak{U}}$$

Para cada $x \in \mathbb{R}$, consideramos x^* como sendo a classe de equivalência da sequência $\langle x \rangle_{i\in\mathbb{N}}$, ou seja, a sequência constante em x.

Análise não standard

Seja $\mathfrak{U}$ um ultrafiltro sobre $\mathbb{N}$ que não contém subconjuntos finitos. e considere, na linguagem de anéis ordenados:

$$\mathcal{M}^* = \frac{\prod_{i\in\mathbb{N}} \mathbb{R}}{\mathfrak{U}}$$

Para cada $x \in \mathbb{R}$, consideramos x^* como sendo a classe de equivalência da sequência $\langle x \rangle_{i\in\mathbb{N}}$, ou seja, a sequência constante em x.
Veja que, se $x < y$, então $x^* < y^*$, pois $\{i \in \mathbb{N} : x < y\} = \mathbb{N}$

Inifinitesimais

Seja $\delta \in \mathcal{M}^*$.
Dizemos que:

- δ é positivo quando $0^* < \delta$;
- δ é infinitesimal quando, para qualquer $x \in \mathbb{R}$ positivo, $-x^* < \delta < x^*$.

Inifinitesimais

Seja $\delta \in \mathcal{M}^*$.
Dizemos que:

- δ é positivo quando $0^* < \delta$;
- δ é infinitesimal quando, para qualquer $x \in \mathbb{R}$ positivo, $-x^* < \delta < x^*$.

Existem infinitesimais positivos?

Inifinitesimais

Seja $\delta \in \mathcal{M}^*$.
Dizemos que:

- δ é positivo quando $0^* < \delta$;
- δ é infinitesimal quando, para qualquer $x \in \mathbb{R}$ positivo, $-x^* < \delta < x^*$.

Existem infinitesimais positivos? Sim!

Infinitesimais positivos

São exemplos de infinitesimais:

- $\left\langle \frac{1}{i} \right\rangle_{i \in \mathbb{N}}$;
- $\left\langle \frac{1}{2^i} \right\rangle_{i \in \mathbb{N}}$.

Infinitesimais positivos

São exemplos de infinitesimais:

- $\left\langle \frac{1}{i} \right\rangle_{i \in \mathbb{N}}$;
- $\left\langle \frac{1}{2^i} \right\rangle_{i \in \mathbb{N}}$.

Pois, para cada $r \in \mathbb{R}$ positivo, tome n grande o suficiente tal que $\frac{1}{n} < r$.
Então, para todo $i > n$ (isto é, uma grande quantidade), $\frac{1}{i} < r$ e, portanto, $\left\langle \frac{1}{i} \right\rangle < r^*$.

Infinitos também

Agora, podem existir números tais que $\frac{1}{x}$ é *infinito*!

Infinitos também

Agora, podem existir números tais que $\frac{1}{x}$ é *infinito*!
Um elemento $\delta \in \mathcal{M}^*$ é dito finito quando $|\delta| < r^*$, para algum $r \in \mathbb{R}$.
Caso contrário, é infinito.

Infinitos também

Agora, podem existir números tais que $\frac{1}{x}$ é *infinito*!
Um elemento $\delta \in \mathcal{M}^*$ é dito finito quando $|\delta| < r^*$, para algum $r \in \mathbb{R}$.
Caso contrário, é infinito.

Por exemplo, $\langle i \rangle_{i \in \mathbb{N}}$ é infinito.

Infinitos também

Agora, podem existir números tais que $\frac{1}{x}$ é *infinito*!
Um elemento $\delta \in \mathcal{M}^*$ é dito finito quando $|\delta| < r^*$, para algum $r \in \mathbb{R}$.
Caso contrário, é infinito.

Por exemplo, $\langle i \rangle_{i \in \mathbb{N}}$ é infinito.

Esses números que construímos são chamados de *hiperreais*.
Existem também os números *surreais*, que vêm a partir de uma construção usando jogos combinatórios e são bem interessantes.

Voltando para a álgebra

Vamos nos concentrar, agora, na teoria de corpos algebricamente fechados.
Antes de passar para as aplicações, vale um comentário sobre polinômios.

Voltando para a álgebra

Vamos nos concentrar, agora, na teoria de corpos algebricamente fechados.
Antes de passar para as aplicações, vale um comentário sobre polinômios.

Como escrevemos um polinômio em lógica de primeira ordem?
Usamos termos com variáveis livres:

$$t(x, a_0, a_1, ..., a_n) = a_0 + a_1x + ... + a_nx^n$$

Voltando para a álgebra

Vamos nos concentrar, agora, na teoria de corpos algebricamente fechados.
Antes de passar para as aplicações, vale um comentário sobre polinômios.

Como escrevemos um polinômio em lógica de primeira ordem?
Usamos termos com variáveis livres:

$$t(x, a_0, a_1, ..., a_n) = a_0 + a_1x + ... + a_nx^n$$

Veja que isso é válido pela construção de termos.

Na verdade, os termos da linguagem de anéis são somas e produtos concatenados, ou seja, são sempre polinômios!
Podemos, também, escrever polinômios com mais de uma variável:

$$t(x_1, x_2, a_{00}, \ldots, a_{nm}) = \sum_{i<n,\, j<m} a_{ij} x_1^i x_2^j$$

Na verdade, os termos da linguagem de anéis são somas e produtos concatenados, ou seja, são sempre polinômios!
Podemos, também, escrever polinômios com mais de uma variável:

$$t(x_1, x_2, a_{00}, \ldots, a_{nm}) = \sum_{i<n,\, j<m} a_{ij} x_1^i x_2^j$$

Além disso, podemos descrever, a partir de fórmulas, funções polinomiais em várias coordenadas:
Considere $f : F^n \to F^n$ uma função polinomial.

Na verdade, os termos da linguagem de anéis são somas e produtos concatenados, ou seja, são sempre polinômios!
Podemos, também, escrever polinômios com mais de uma variável:

$$t(x_1, x_2, a_{00}, \ldots, a_{nm}) = \sum_{i<n,\, j<m} a_{ij} x_1^i x_2^j$$

Além disso, podemos descrever, a partir de fórmulas, funções polinomiais em várias coordenadas:
Considere $f : F^n \to F^n$ uma função polinomial.
Ou seja, em cada coordenada, f é um polinômio. Sejam $\overline{x}$ e $\overline{y}$ n-uplas. Dizemos que $f(\overline{x}) = \overline{y}$ quando, para cada i, $f_i(\overline{x}) = y_i$.

Isto é, em cada coordenada i, f é um polinômio de n variáveis. Cada uma dessas coordenadas, então, pode ser representada por um termo, como vimos anteriormente:

$$t_i(x_1, x_2, \ldots, x_n, \overline{a_i})$$

sendo $\overline{a_i}$ os coeficientes de f_i.

Isto é, em cada coordenada i, f é um polinômio de n variáveis. Cada uma dessas coordenadas, então, pode ser representada por um termo, como vimos anteriormente:

$$t_i(x_1, x_2, ..., x_n, \overline{a_i})$$

sendo $\overline{a_i}$ os coeficientes de f_i.

Nesse caso, $f(\overline{x}) = \overline{y}$ se traduz, em lógica de primeira ordem, a:

$$\varphi(\overline{x}, \overline{y}, \overline{a_1}, \overline{a_2}, ..., \overline{a_n}) \equiv \bigwedge_{1 \leq i \leq n} t_i(\overline{x}, \overline{a_i}) = y_i$$

Um teorema

Precisamos disso para compreender que é possível descrever o seguinte problema em lógica de primeira ordem:

Teorema (Ax-Grothendieck)

Se uma função polinomial $f : \mathbb{C}^n \to \mathbb{C}^n$ é injetora, então é sobrejetora.

Um teorema

Precisamos disso para compreender que é possível descrever o seguinte problema em lógica de primeira ordem:

Teorema (Ax-Grothendieck)

Se uma função polinomial $f : \mathbb{C}^n \to \mathbb{C}^n$ é injetora, então é sobrejetora.

Veja que também precisaremos de sentenças atestando injetividade e sobrejetividade.
Vamos resolver esse problema de vez.

Sobrejetividade e injetividade

Seja $\varphi(\overline{x}, \overline{y}, \overline{a})$ uma fórmula que representa uma função polinomial f em n coordenadas.

- f é injetiva: $\forall \overline{x}_1 \forall \overline{x}_2 (\overline{x}_1 \neq \overline{x}_2 \rightarrow (\neg \exists \overline{y}\, \varphi(\overline{x}_1, \overline{y}, \overline{a}) \wedge \varphi(\overline{x}_2, \overline{y}, \overline{a})))$;
- f é sobrejetiva: $\forall \overline{y} \exists \overline{x} \varphi(\overline{x}, \overline{y}, \overline{a})$.

Sobrejetividade e injetividade

Seja $\varphi(\overline{x}, \overline{y}, \overline{a})$ uma fórmula que representa uma função polinomial f em n coordenadas.

- f é injetiva: $\forall \overline{x}_1 \forall \overline{x}_2 (\overline{x}_1 \neq \overline{x}_2 \rightarrow (\neg \exists \overline{y}\, \varphi(\overline{x}_1, \overline{y}, \overline{a}) \wedge \varphi(\overline{x}_2, \overline{y}, \overline{a})))$;
- f é sobrejetiva: $\forall \overline{y} \exists \overline{x} \varphi(\overline{x}, \overline{y}, \overline{a})$.

Veja que tomamos alguns atalhos, como usar $\overline{a} = \overline{b}$ em vez de $a_1 = b_1 \wedge \ldots \wedge a_n = b_n$ e $\exists \overline{x}$ em vez de $\exists x_1 \exists x_2 \ldots \exists x_n$.

Sobrejetividade e injetividade

Seja $\varphi(\overline{x}, \overline{y}, \overline{a})$ uma fórmula que representa uma função polinomial f em n coordenadas.

- f é injetiva: $\forall \overline{x}_1 \forall \overline{x}_2 (\overline{x}_1 \neq \overline{x}_2 \rightarrow (\neg \exists \overline{y}\, \varphi(\overline{x}_1, \overline{y}, \overline{a}) \wedge \varphi(\overline{x}_2, \overline{y}, \overline{a})))$;
- f é sobrejetiva: $\forall \overline{y} \exists \overline{x} \varphi(\overline{x}, \overline{y}, \overline{a})$.

Veja que tomamos alguns atalhos, como usar $\overline{a} = \overline{b}$ em vez de $a_1 = b_1 \wedge ... \wedge a_n = b_n$ e $\exists \overline{x}$ em vez de $\exists x_1 \exists x_2 ... \exists x_n$.

Se quisermos carregar a notação inteira o tempo todo, fica impossível de administrar.

Trocando de corpo

Para provar o teorema, a técnica que vamos usar será não provar o resultado usando o corpo $\mathbb{C}$ diretamente, mas um ultraproduto que nos permite trabalhar com corpos finitos.

Trocando de corpo

Para provar o teorema, a técnica que vamos usar será não provar o resultado usando o corpo $\mathbb{C}$ diretamente, mas um ultraproduto que nos permite trabalhar com corpos finitos.

Seja $\mathbb{F}_p$ um corpo finito. Consideramos $\overline{\mathbb{F}_p}$ o fecho algébrico de $\mathbb{F}_p$

Trocando de corpo

Para provar o teorema, a técnica que vamos usar será não provar o resultado usando o corpo $\mathbb{C}$ diretamente, mas um ultraproduto que nos permite trabalhar com corpos finitos.

Seja $\mathbb{F}_p$ um corpo finito. Consideramos $\overline{\mathbb{F}_p}$ o fecho algébrico de $\mathbb{F}_p$ Queremos mostrar que o ultraproduto dos $\overline{\mathbb{F}_p}$ é isomorfo a $\mathbb{C}$.

Trocando de corpo

Para provar o teorema, a técnica que vamos usar será não provar o resultado usando o corpo $\mathbb{C}$ diretamente, mas um ultraproduto que nos permite trabalhar com corpos finitos.

Seja $\mathbb{F}_p$ um corpo finito. Consideramos $\overline{\mathbb{F}_p}$ o fecho algébrico de $\mathbb{F}_p$ Queremos mostrar que o ultraproduto dos $\overline{\mathbb{F}_p}$ é isomorfo a $\mathbb{C}$. Para isso, vamos mostrar que o ultraproduto é um corpo algebricamente fechado de cardinalidade $\mathfrak{c} = 2^\omega$ e característica 0, portanto, como ACF_0 é categórica para todo cardinal não enumerável, o ultraproduto deve ser isomorfo aos complexos.

Como cada $\overline{\mathbb{F}_p}$ é um modelo para ACF, o ultraproduto também será. Pelo Teorema de Łoś, para cada sentença $\varphi \in ACF$, todo $\overline{\mathbb{F}_p} \models \varphi$, portanto $\mathcal{M}^* \models \varphi$.

Como cada $\overline{\mathbb{F}_p}$ é um modelo para ACF, o ultraproduto também será. Pelo Teorema de Łoś, para cada sentença $\varphi \in ACF$, todo $\overline{\mathbb{F}_p} \models \varphi$, portanto $\mathcal{M}^* \models \varphi$.

Além disso, a característica é 0, pois não pode ser positiva (pelo argumento que fizemos ontem).

Como cada $\overline{\mathbb{F}_p}$ é um modelo para ACF, o ultraproduto também será. Pelo Teorema de Łoś, para cada sentença $\varphi \in ACF$, todo $\overline{\mathbb{F}_p} \models \varphi$, portanto $\mathcal{M}^* \models \varphi$.

Além disso, a característica é 0, pois não pode ser positiva (pelo argumento que fizemos ontem).

Resta mostrar que a cardinalidae é 2^ω.

Para isso, primeiro lembre que a cardinalidade de ω^ω e 2^ω é igual.
Veja que o ultraproduto é um produtório de enumeráveis conjuntos enumeráveis quocientado por uma relação de equivalência.
Temos que a cardinalidade máxima é a de ω^ω (que é a cardinalidade antes do quociente). Vamos mostrar que o conjunto não é menor que ω^ω.

Para isso, primeiro lembre que a cardinalidade de ω^ω e 2^ω é igual.
Veja que o ultraproduto é um produtório de enumeráveis conjuntos enumeráveis quocientado por uma relação de equivalência.
Temos que a cardinalidade máxima é a de ω^ω (que é a cardinalidade antes do quociente). Vamos mostrar que o conjunto não é menor que ω^ω.

Na verdade não vamos.
É um argumento de combinatória infinita e você pode ler a prova em `https://math.stackexchange.com/questions/1417688/cardinality-of-ultraproduct`

Provando o Teorema

Queremos provar: uma função polinomial $f : \mathbb{C}^n \to \mathbb{C}^n$ é injetiva somente se é sobrejetiva.

Provando o Teorema

Queremos provar: uma função polinomial $f : \mathbb{C}^n \to \mathbb{C}^n$ é injetiva somente se é sobrejetiva.

Conseguimos descrever o gráfico de f por uma fórmula $\varphi(\overline{x}, \overline{y}, \overline{a})$ e conseguimos uma fórmula $\psi(\overline{a})$ que diz que f é injetiva mas não sobrejetiva.

Provando o Teorema

Queremos provar: uma função polinomial $f : \mathbb{C}^n \to \mathbb{C}^n$ é injetiva somente se é sobrejetiva.

Conseguimos descrever o gráfico de f por uma fórmula $\varphi(\overline{x}, \overline{y}, \overline{a})$ e conseguimos uma fórmula $\psi(\overline{a})$ que diz que f é injetiva mas não sobrejetiva.

Suponha o resultado falso. Então, existem coeficientes $\overline{b} \in \mathbb{C}$ tais que $\mathbb{C} \models \psi(\overline{b})$.

Provando o Teorema

Queremos provar: uma função polinomial $f : \mathbb{C}^n \to \mathbb{C}^n$ é injetiva somente se é sobrejetiva.

Conseguimos descrever o gráfico de f por uma fórmula $\varphi(\overline{x}, \overline{y}, \overline{a})$ e conseguimos uma fórmula $\psi(\overline{a})$ que diz que f é injetiva mas não sobrejetiva.

Suponha o resultado falso. Então, existem coeficientes $\overline{b} \in \mathbb{C}$ tais que $\mathbb{C} \models \psi(\overline{b})$.
Isto é, $\mathbb{C} \models \exists \overline{z}\ \psi(\overline{z})$.

Pelo teorema de Łoś, para muitos primos p, $\overline{\mathbb{F}_p} \models \exists \overline{z}\ \psi(\overline{z})$.
Em particular, isso é satisfeito para um primo q.

Pelo teorema de Łoś, para muitos primos p, $\overline{\mathbb{F}_p} \models \exists \bar{z}\ \psi(\bar{z})$.
Em particular, isso é satisfeito para um primo q.

Ou seja, $\overline{\mathbb{F}_q} \models \exists \bar{z} \psi(\bar{z})$.
Isso significa que existe uma função polinomial $g : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ que é injetiva mas não sobrejetiva.

Pelo teorema de Łoś, para muitos primos p, $\overline{\mathbb{F}_p} \models \exists \overline{z}\ \psi(\overline{z})$.
Em particular, isso é satisfeito para um primo q.

Ou seja, $\overline{\mathbb{F}_q} \models \exists \overline{z} \psi(\overline{z})$.
Isso significa que existe uma função polinomial $g : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ que é injetiva mas não sobrejetiva.

Seja $\overline{y} \subset \overline{\mathbb{F}_q}$ tal que não existe $\overline{x}$ de modo que $g(\overline{x}) = \overline{y}$.
Seja $\mathbb{F}_s$ uma extensão de $\mathbb{F}_q$ grande o suficiente para conter todos os coeficientes de g e também os elementos de y.

Veja, então, que a restrição de g a $\mathbb{F}_s^n$ é polinomial e, portanto, sua imagem está contida em $\mathbb{F}_s^n$.
Além disso, a restrição de uma função injetiva continua injetiva.

Veja, então, que a restrição de g a $\mathbb{F}_s^n$ é polinomial e, portanto, sua imagem está contida em $\mathbb{F}_s^n$.
Além disso, a restrição de uma função injetiva continua injetiva.

Mas veja: se temos uma função injetiva $\gamma : X \to Y$, então $|X| = |\gamma(X)|$.
Desse modo, $|g(\mathbb{F}_s^n)| = |\mathbb{F}_s^n|$.

Veja, então, que a restrição de g a $\mathbb{F}_s^n$ é polinomial e, portanto, sua imagem está contida em $\mathbb{F}_s^n$.
Além disso, a restrição de uma função injetiva continua injetiva.

Mas veja: se temos uma função injetiva $\gamma : X \to Y$, então $|X| = |\gamma(X)|$.
Desse modo, $|g(\mathbb{F}_s^n)| = |\mathbb{F}_s^n|$.

Mas o único subconjunto de $\mathbb{F}_s^n$ com a mesma cardinalidade que ele mesmo é o conjunto inteiro, porque é finito.
Portanto, $g : \mathbb{F}_s^n \to \mathbb{F}_s^n$ é sobrejetiva.

Veja, então, que a restrição de g a $\mathbb{F}_s^n$ é polinomial e, portanto, sua imagem está contida em $\mathbb{F}_s^n$.
Além disso, a restrição de uma função injetiva continua injetiva.

Mas veja: se temos uma função injetiva $\gamma : X \to Y$, então $|X| = |\gamma(X)|$.
Desse modo, $|g(\mathbb{F}_s^n)| = |\mathbb{F}_s^n|$.

Mas o único subconjunto de $\mathbb{F}_s^n$ com a mesma cardinalidade que ele mesmo é o conjunto inteiro, porque é finito.
Portanto, $g : \mathbb{F}_s^n \to \mathbb{F}_s^n$ é sobrejetiva.
Em particular, existe $\overline{x}$ tal que $g(\overline{x}) = \overline{y}$.

Isomorfismo e equivalência

Não provamos que o ultraproduto é, de fato, isomorfo a $\mathbb{C}$, mas você pode perceber que isso sequer é necessário.
Como, para cada p, a teoria ACF_p é categórica para cardinais não enumeráveis, então ela é completa:

Isomorfismo e equivalência

Não provamos que o ultraproduto é, de fato, isomorfo a $\mathbb{C}$, mas você pode perceber que isso sequer é necessário.
Como, para cada p, a teoria ACF_p é categórica para cardinais não enumeráveis, então ela é completa:

Suponha que não e sejam $\mathcal{M}$ e $\mathcal{N}$ dois modelos para ACF_p.
Usando os teoremas de Löwenheim-Skolem, conseguimos $\mathcal{M}'$ e $\mathcal{N}'$ modelos de cardinalidade κ (um cardinal não enumerável qualquer) tais que:

- $\mathcal{M}' \equiv \mathcal{M}$;
- $\mathcal{N}' \equiv \mathcal{N}$;

Como ACF_p é κ-categórica, então $\mathcal{M}' \simeq \mathcal{N}'$.
Em particular, $\mathcal{M}' \equiv \mathcal{N}'$.

Como ACF_p é κ-categórica, então $\mathcal{M}' \simeq \mathcal{N}'$.
Em particular, $\mathcal{M}' \equiv \mathcal{N}'$.

Portanto,

$$\mathcal{M} \equiv \mathcal{M}' \equiv \mathcal{N}' \equiv \mathcal{N}$$

Como ACF_p é κ-categórica, então $\mathcal{M}' \simeq \mathcal{N}'$.
Em particular, $\mathcal{M}' \equiv \mathcal{N}'$.

Portanto,

$$\mathcal{M} \equiv \mathcal{M}' \equiv \mathcal{N}' \equiv \mathcal{N}$$

Como, para provar o teorema, usamos apenas sentenças, não dependemos de valoração, isto é, o isomorfismo não é necessário.

Irreducibilidade de polinômios

Teorema

Seja f um polinômio com coeficientes inteiros. Considere, para um dado p, f_p o polinômio f com os coeficientes tomados módulo p. Então, f é irredutível em $\mathbb{C}$ se e somente se, para a maioria dos $\overline{\mathbb{F}_p}$, f_p é irredutível.

Irreducibilidade de polinômios

Teorema

Seja f um polinômio com coeficientes inteiros. Considere, para um dado p, f_p o polinômio f com os coeficientes tomados módulo p. Então, f é irredutível em $\mathbb{C}$ se e somente se, para a maioria dos $\overline{\mathbb{F}_p}$, f_p é irredutível.

Note que números inteiros podem ser descritos sem precisar de valoração, isto é, apenas a partir de termos livres de variáveis. Isso é verdade pois $n = \underbrace{1 + 1 + \ldots + 1}_{n \text{ vezes}}$.

Irreducibilidade de polinômios

Teorema

Seja f um polinômio com coeficientes inteiros. Considere, para um dado p, f_p o polinômio f com os coeficientes tomados módulo p. Então, f é irredutível em $\mathbb{C}$ se e somente se, para a maioria dos $\overline{\mathbb{F}_p}$, f_p é irredutível.

Note que números inteiros podem ser descritos sem precisar de valoração, isto é, apenas a partir de termos livres de variáveis. Isso é verdade pois $n = \underbrace{1 + 1 + ... + 1}_{n \text{ vezes}}$.

Veja, então, que a redução de um inteiro módulo p ocorre naturalmente pela interpretação do corpo de característica positiva, sem precisar "mexer"nos coeficientes.

Assim, o gráfico de um polinômio com coeficientes inteiros pode ser definido por uma fórmula $\varphi(x, y)$.

Assim, o gráfico de um polinômio com coeficientes inteiros pode ser definido por uma fórmula $\varphi(x, y)$.

Se conseguirmos traduzir "f é irredutível"para uma sentença, então o nosso problema terá acabado, por causa do Teorema de Łoś, que garante que uma sentença de primeira ordem é válida em $\mathbb{C}$ se e somente se é válida na maioria dos $\overline{\mathbb{F}_p}$.

Reducibilidade

Vamos mostrar que a reducibilidade é descritível em primeira ordem. Temos f um polinômio de grau n com coeficientes inteiros e $\varphi(x, y)$ a fórmula representando seu gráfico.

Reducibilidade

Vamos mostrar que a reducibilidade é descritível em primeira ordem.
Temos f um polinômio de grau n com coeficientes inteiros e $\varphi(x, y)$ a fórmula representando seu gráfico.

Um polinômio é redutível quando é produto de dois polinômios de menor grau.
Suponhamos que $f = gh$, com gh não necessariamente com coeficientes inteiros.

$$g(x) = a_0 + a_1 x + \ldots + a_n x^n$$

$$h(x) = b_0 + b_1 x + \ldots + b_n x^n$$

$$g(x) = a_0 + a_1 x + ... + a_n x^n$$

$$h(x) = b_0 + b_1 x + ... + b_n x^n$$

Descrevemos o gráfico de g e h como:

- $\psi(x, y, \overline{a})$;
- $\psi(x, y, \overline{b})$;

Observe que ψ é um esqueleto para um polinômio:

$$\psi(x, y, a_0, ..., a_n) \equiv a_0 + a_1 x + ... + a_n x^n = y$$

Mudando os coeficientes $\overline{a}$ e $\overline{b}$, teremos todas as possibilidades de fatores para f.

Observe que ψ é um esqueleto para um polinômio:

$$\psi(x, y, a_0, ..., a_n) \equiv a_0 + a_1 x + ... + a_n x^n = y$$

Mudando os coeficientes $\overline{a}$ e $\overline{b}$, teremos todas as possibilidades de fatores para f. Isso ocorre porque f não pode se fatorar em polinômios de grau maior que o seu próprio grau.

Observe que ψ é um esqueleto para um polinômio:

$$\psi(x, y, a_0, ..., a_n) \equiv a_0 + a_1 x + ... + a_n x^n = y$$

Mudando os coeficientes $\overline{a}$ e $\overline{b}$, teremos todas as possibilidades de fatores para f. Isso ocorre porque f não pode se fatorar em polinômios de grau maior que o seu próprio grau.
Dizer que $f = gh$ é dizer que, para todo x, $f(x) = g(x) \times h(x)$.
Podemos traduzir isso para primeira ordem como:

$$\forall x \forall y (\varphi(x, y) \leftrightarrow \exists y_1 \exists y_2 (\psi(x, y_1, \overline{a}) \wedge \psi(x, y_2, \overline{b}) \wedge y = y_1 \times y_2))$$

Portanto, a seguinte fórmula diz que f é irredutível:

$$\nexists \overline{a}\ \nexists \overline{b} \forall x \forall y (\varphi(x,y) \leftrightarrow \exists y_1 \exists y_2 (\psi(x,y_1,\overline{a}) \wedge \psi(x,y_2,\overline{b}) \wedge y = y_1 \times y_2))$$

Portanto, a seguinte fórmula diz que f é irredutível:

$$\nexists \overline{a}\ \nexists \overline{b} \forall x \forall y (\varphi(x,y) \leftrightarrow \exists y_1 \exists y_2 (\psi(x,y_1,\overline{a}) \wedge \psi(x,y_2,\overline{b}) \wedge y = y_1 \times y_2))$$

Precisaríamos adicionar condições para impedir que os fatores sejam triviais (como $1 \times f$).
Mas, nesse caso, a sentença ficaria grande demais. Não é difícil, no entanto, acrescentar essas condições à sentença.

Portanto, a seguinte fórmula diz que f é irredutível:

$$\nexists \overline{a} \ \nexists \overline{b} \forall x \forall y (\varphi(x,y) \leftrightarrow \exists y_1 \exists y_2 (\psi(x,y_1,\overline{a}) \wedge \psi(x,y_2,\overline{b}) \wedge y = y_1 \times y_2))$$

Precisaríamos adicionar condições para impedir que os fatores sejam triviais (como $1 \times f$).
Mas, nesse caso, a sentença ficaria grande demais. Não é difícil, no entanto, acrescentar essas condições à sentença.

Veja, que, agora, a fórmula se tornou uma sentença: não há variáveis livres.
Podemos, então, usar o Teorema de Łoś e obter o resultado desejado.

Do finito ao infinito...

O primeiro resultado que fizemos nos permite usar corpos finitos para obter uma propriedade sobre $\mathbb{C}$.
Usando ultraprodutos, também é possível obter resultados que fazem o caminho oposto.

Do finito ao infinito...

O primeiro resultado que fizemos nos permite usar corpos finitos para obter uma propriedade sobre $\mathbb{C}$.
Usando ultraprodutos, também é possível obter resultados que fazem o caminho oposto.
Isto é, conhecendo uma propriedade sobre uma estrutura infinita, obter algo sobre estrutura finitas.

Os teoremas de Ramsey

Dado grafo G, uma coloração de G em n cores é uma função que leva as arestas de G em $\{1, 2, ..., n\}$.
Isto é, uma função que "pinta"cada aresta de uma cor.

Os teoremas de Ramsey

Dado grafo G, uma coloração de G em n cores é uma função que leva as arestas de G em $\{1, 2, ..., n\}$.
Isto é, uma função que "pinta"cada aresta de uma cor.
Vamos nos preocupar apenas com o caso mais simples: de duas cores.

Os teoremas de Ramsey

Dado grafo G, uma coloração de G em n cores é uma função que leva as arestas de G em $\{1, 2, ..., n\}$.
Isto é, uma função que "pinta"cada aresta de uma cor.
Vamos nos preocupar apenas com o caso mais simples: de duas cores.

Em vez de usar a linguagem $\{E\}$ para grafos, como normalmente, usamos uma linguagem diferente: $\{V, A\}$, isto é:

- $A(x, y)$ se os vértices x e y estão ligados por uma aresta azul;
- $V(x, y)$ se os vértices x e y estão ligados por uma aresta vermelha.

Teorema

Dado um grafo infinito e completo G, para qualquer coloração de suas arestas em azul e vermelho, há um subconjunto infinito do grafo tal que todos os vértices estão ligados pela mesma cor.

Teorema

Dado um grafo infinito e completo G, para qualquer coloração de suas arestas em azul e vermelho, há um subconjunto infinito do grafo tal que todos os vértices estão ligados pela mesma cor.

Nessa nova linguagem, o grafo ser completo significa que $\forall x \forall y \ (x \neq y \rightarrow (V(x,y) \vee A(x,y)))$.
Além disso, uma aresta não pode ter duas cores, então $\forall x \forall y \neg (A(x,y) \wedge V(x,y))$.

Versão finita

Teorema

Para cada n, existe um M grande o suficiente tal que toda coloração de um grafo completo com M vértices admite um subconjunto com n vértices tal que todos estão ligados por arestas de mesma cor.

Versão finita

Teorema

Para cada n, existe um M grande o suficiente tal que toda coloração de um grafo completo com M vértices admite um subconjunto com n vértices tal que todos estão ligados por arestas de mesma cor.

Suponha o resultado falso para um n qualquer.
Isto é, para cada M, existe um grafo completo G_M, com M vértices, com uma coloração em azul e vermelho de modo que nenhum subconjunto de n vértices é homogêneo.
Façamos o ultraproduto de todos os G_M.

Como vimos anteriormente, o ultraproduto de todos os grafos completos finitos é um grafo completo infinito.
Neste caso, a nossa linguagem já traz a coloração, portanto o grafo infinito terá as arestas coloridas com as cores azul e vermelho.

Como vimos anteriormente, o ultraproduto de todos os grafos completos finitos é um grafo completo infinito.
Neste caso, a nossa linguagem já traz a coloração, portanto o grafo infinito terá as arestas coloridas com as cores azul e vermelho.

Sabemos, pela versão infinita do teorema, que esse grafo tem um subconjunto infinito cujas arestas têm todas a mesma cor.
Em particular, há um subonjunto de n vértices tal que todas têm a mesma cor.

Como vimos anteriormente, o ultraproduto de todos os grafos completos finitos é um grafo completo infinito.
Neste caso, a nossa linguagem já traz a coloração, portanto o grafo infinito terá as arestas coloridas com as cores azul e vermelho.

Sabemos, pela versão infinita do teorema, que esse grafo tem um subconjunto infinito cujas arestas têm todas a mesma cor.
Em particular, há um subonjunto de n vértices tal que todas têm a mesma cor.

A propriedade "existem n vértices cujas arestas entre eles têm a mesma cor"pode ser descrita como uma sentença em lógica de primeira ordem.
Agora, o ultraproduto satisfaz a sentença mas nenhum dos G_M a satisfaz: pelo Teorema de Łoś, isso é uma contradição.

Como vimos anteriormente, o ultraproduto de todos os grafos completos finitos é um grafo completo infinito.
Neste caso, a nossa linguagem já traz a coloração, portanto o grafo infinito terá as arestas coloridas com as cores azul e vermelho.

Sabemos, pela versão infinita do teorema, que esse grafo tem um subconjunto infinito cujas arestas têm todas a mesma cor.
Em particular, há um subonjunto de n vértices tal que todas têm a mesma cor.

A propriedade "existem n vértices cujas arestas entre eles têm a mesma cor"pode ser descrita como uma sentença em lógica de primeira ordem.
Agora, o ultraproduto satisfaz a sentença mas nenhum dos G_M a satisfaz: pelo Teorema de Łoś, isso é uma contradição.

O resultado segue.

Até amanhã!