حذف سور و تصمیم‌پذیری

سخنرانی روز جبر ـ خانه ریاضیات

محسن خانی

۲۱ آذر ۱۴۰۳

اواسط فیلم: تعریف‌پذیری

- در $\langle \mathbb{R}, +, \cdot \rangle$ بگو $x < y$:

$$\exists z \quad x = y + z^2.$$

- در $\langle \mathbb{Z}, +, \cdot \rangle$ بگو $x < y$:

$$\exists z_1, z_2, z_3, z_4 \quad y = x + z_1^2 + z_2^2 + z_3^2 + z_4^2. \quad \text{قضیه لاگرانژ}$$

- در $\langle \mathbb{N}, + \rangle$ بگو $x < y$:

$$\exists z \quad x + z = y$$

- در $\langle \mathbb{Z}, + \rangle$ بگو $x < y$:

نمی‌توانم!

- (ژولیا رابینسون) در $\langle \mathbb{Q}, +, \cdot \rangle$ بگو $x \in \mathbb{Z}$ (صفحه بعد!)
- در $\langle \mathbb{C}, +, \cdot \rangle$ بگو $x \in \mathbb{R}$ یا بگو $x \in \mathbb{Z}$.

نمی‌توانم!

- (انواع و اقسام سوالات) در حلقهٔ $\mathbb{Q}_{(p)}$ بگو $x \in \mathbb{Z}_{(p)}$. در یک میدان ارزیابی بگو $v(x) > 0$ و ... .

فرمول ژولیا رابینسون برای تعریف $\mathbb{Z}$ در $\mathbb{Q}$:

DEFINABILITY AND DECISION PROBLEMS IN ARITHMETIC 107

$$\bigwedge_{A,B} \Big(\Big\{\Big(\bigvee_{X,Y,Z} 2 + BZ^2 = X^2 + AY^2\Big) \wedge \bigwedge_{M} \Big[\Big(\bigvee_{X,Y,Z} 2 + ABM^2 + BZ^2 = X^2 + AY^2\Big) \rightarrow \Big(\bigvee_{X,Y,Z} 2 + AB(M+1)^2 + BZ^2 = X^2 + AY^2\Big)\Big]\Big\} \rightarrow \Big(\bigvee_{X,Y,Z} 2 + ABN^2 + BZ^2 = X^2 + AY^2\Big)\Big).$$

توجه. اخیراً فرمول‌های با پیچیدگی کمتر ارائه شده است:
Koenigsmann, J. (2016). Defining Z in Q. Annals of Mathematics, 73-93.

در $\langle \mathbb{N}, +, \cdot \rangle$ می‌توانم این جمله را بگویم که

$$\varphi(m, n) \iff \text{الگوریتم شماره } m \text{ در ورودی } n \text{ بایستد}$$

دسته‌بندی شلاه ۱۹۷۸

تئوری T:

- ویژگی ترتیبی دارد هرگاه یک فرمول $\varphi(x, y)$ و دو دنبالهٔ (a_i) و (b_j) وجود داشته باشند به طوری که

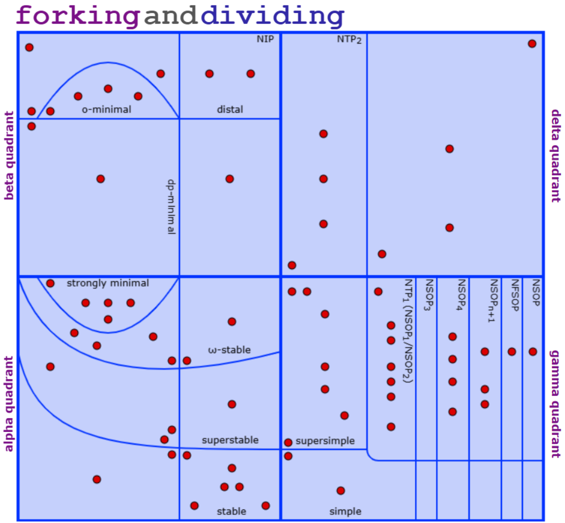
$$\varphi(a_i, b_j) \iff i < j.$$

- تئوری T ویژگی وابستگی دارد هر گاه یک فرمول $\varphi(x, y)$ و دو دنباله (a_i) و (b_J) وجود داشته باشند که

$$\varphi(a_i, b_J) \iff i \in J.$$

- کاملاً متعالی است هرگاه هیچ فرمولی درخت نسازد!
- ....
- تئوری‌های وابسته، دارای ویژگی درختی، دارای ویژگی ترتیبی و ... .

نقشه جهان



Map of the Universe

Nice Properties of Theories

ω-stable	superstable	stable	
strongly minimal	dp-minimal	o-minimal	
supersimple	simple	NIP	distal
NTP$_1$ (NSOP$_1$/NSOP$_2$)	NTP$_2$	NSOP	
NSOP$_3$	NSOP$_4$	NSOP$_{n+1}$	NFSOP

Click a property above to highlight region and display details. Or click the map for specific region information.

Reset

List of Examples

- ACF
- $\mathbb{Q}$-vector spaces
- $(\mathbb{Z}, x \mapsto x+1)$
- Hrushovski's new strongly minimal set
- infinite sets
- everywhere infinite forest
- infinitely expanding equivalence relations
- Farey graph
- $((\mathbb{Z}/4\mathbb{Z})^{\omega}, +)$
- DCF$_0$

Implications Between Properties

Open Regions

Open Examples

قصه از کجا شروع شد...
از گل و باغ و جووونه؟!

(تمامیت گودل) فرض کنید T یک مجموعه از اصول موضوعه باشد و φ یک جمله باشد.

$$T \vdash \varphi \iff T \cup \{\neg\varphi\} \text{ هیچ مدلی نداشته باشد}$$

نتیجه

چه زمانی یک مدل برای یک مجموعه از اصول موضوعه وجود دارد؟

احتمالا باید مدل‌های کوچک را با هم **ادغام** کنیم.

امکان دارد که

$$T \nvdash \varphi \quad T \nvdash \neg\varphi.$$

یعنی این گونه نیست که

$$T \nvdash \varphi \iff T \vdash \neg\varphi.$$

تعریف

- می‌گوییم T یک تئوری تصمیم‌پذیر است هرگاه یک الگوریتم وجود داشته باشد که یک جملهٔ φ را بگیرد و تعیین کند که آیا $T \vdash \varphi$ یا $T \nvdash \varphi$.
- می‌گوییم تئوری T کامل است هرگاه از $T \nvdash \varphi$ نتیجه شود که $T \vdash \neg\varphi$.

ادغام ساختارها

- $\bigoplus_{i\in I} G_i$: حاصل جمع مستقیم گروه‌ها
- آیا حاصل جمع مستقیم میدان‌ها معنی دارد؟
- ساختاری که به روش خاصی از ساختارهای دیگر به دست می‌آید، چه شباهتهایی با ساختار اولیه دارد؟

فراضرب ساختارها

- فرض کنید $\{M_i\}_{i\in I}$ یک خانواده از ساختارها باشد. حاصل ضرب همهٔ آنها را با M نشان دهید:

$$M = \prod_{i\in I} M_i$$

- I فرض کنید F یک فیلتر روی مجموعه اندیس I باشد. در این صورت F شامل برخی زیرمجموعه‌های I است.
- دو عنصر $\mathbf{a} = (a_i)_{i\in I}$ و $\mathbf{b} = (b_i)_{i\in I}$ را با هم یکی بگیرید در صورتی که

$$\{i \in I : a_i = b_i\} \in F.$$

قضیه (واش)

فراضرب یک خانواده از ساختارها، ویژگی‌های مشترک همهٔ آنها را داراست:

$$M \models \varphi(\mathbf{a}, \mathbf{b}) \iff \{i : M_i \models \varphi(a_i, b_i)\} \in F.$$

میدان سودومتناهی ـ گروه سودومتناهی: اشتراک ویژگی‌های میدانها و گروه‌ها متناهی.

- قضیهٔ فشردگی: فرض کنید T یک تئوری باشد. اگر هر بخش متناهی $\Delta \subseteq T$ دارای مدل باشد، آنگاه T دارای مدل است:

$$M_\Delta \models \Delta \qquad \prod_F M_\Delta \models T$$

$$A_\varphi = \{\Delta : \varphi \in \Delta\} \in F$$

نتایج

- (لونهایم ـ اسکولم) اگر یک تئوری مدل‌های متناهی به اندازه دلخواه بزرگ داشته باشد، آنگاه برای کاردینال دلخواه κ مدلی با اندازه κ دارد.
- اگر φ در میدانهای متناهی با اندازه دلخواه بزرگ درست باشد در $\mathbb{C}$ درست است.
- به عنوان مثال، اکس: هر نگاشت چندجمله‌ای از $\mathbb{C}^n \to \mathbb{C}^n$ اگر یک به یک باشد، پوشاست. (برای یک میدان متناهی این قضیه واضح است!)

بازی

$$
\begin{tikzcd}
x & M & & N & y? \\
 & A \arrow[u] \arrow[r, phantom, "\cong"] & {} \arrow[r, phantom] & B \arrow[u] &
\end{tikzcd}
$$

$$A\langle x\rangle \cong B\langle ?\rangle.$$

قضیه

اگر بازی فوق انجام پذیر باشد، از نظر T برای هر فرمول φ یک معادل بدون سور ψ وجود دارد؛ یعنی

$$T \vdash (\varphi \leftrightarrow \psi).$$

$$\exists x \quad ax^2 + bc + c = 0 \leftrightarrow b^2 - 4ac > 0.$$

مثال: در **میدانهای بسته جبری**، و در **میدانهای بستهٔ حقیقی** می‌توان این بازی را انجام داد.

قضیه ریشه‌ها

قضیه

فرض کنید $I, J \subseteq K[X_1, \ldots, X_n]$ دو ایده‌آل رادیکال باشند به طوری که $J \subsetneq I$. در این صورت $V(I) \subsetneq V(J)$.

اثبات.

$$g \in J - I$$

$$I = p_1 \cap \ldots \cap p_n, \quad I = \langle f_1, \ldots, f_n \rangle$$

$$g \notin p_1 \Rightarrow \frac{K[X]}{p_1} \models g(X) \neq 0$$

$$g \in I \Rightarrow \frac{K[X]}{p_1} \models f_1(X) = \ldots = f_n(X) = 0.$$

$$\frac{K[\bar{X}]}{p_1} \models \exists X \quad f_1(X) = \ldots f_n(X) = 0 \wedge g(X) \neq 0$$

$$K \models \exists x \quad f_1(x) = \ldots, f_n(x) = 0 \wedge g(x) \neq 0.$$

مسئله هفدهم هیلبرت

فرض کنید $f \in K[\bar{X}]$ یک چندجمله‌ای باشد که برای هر $\bar{a}$ داشته باشیم $f(\bar{a}) \geq 0$.
در این صورت

$$f = g_1^2 + \dots g_k^2$$

که در آن g_i ها توابع گویا هستند.

اثبات.
اگر $f \in K[\bar{X}]$ جمع توان دو ها نباشد، یک ترتیب روی $K[\bar{X}]$ داریم که با آن ترتیب $f < 0$. داریم

$$K[\bar{X}] \models \exists \bar{X} \quad f(\bar{X}) < 0 \Rightarrow K \models \exists \bar{x} \quad f(\bar{x}) < 0.$$

□

حذف سور و کامل بودن

فرض کنید تئوری T حذف سور داشته باشد و یک مدل داشته باشد که در تمام مدلهای T می‌نشیند:

$$\begin{tikzcd} M_1 & & M_2 \\ & A \arrow[ul] \arrow[ur] & \end{tikzcd}$$

در این صورت برای هر جمله φ داریم

$$M_1 \models \varphi \iff A \models \varphi \iff M_2 \models \varphi.$$

یعنی برای هر جمله φ داریم

$$T \vdash \varphi \quad \text{یا} \quad T \vdash \neg\varphi$$

محک تصمیم‌پذیری

فرض کنید که یک الگوریتم جملات تئوری T را چاپ کند. این الگوریتم می‌تواند نتایج T را چاپ کند. پس اگر T کامل باشد، در این صورت T تصمیم‌پذیر است.

نتیجه

اگر T حذف سور و مدل اول داشته باشد و اصول موضوعه‌اش توسط الگوریتم قابل چاپ باشد، تصمیم‌پذیر است.

یادآوری: تئوری $(\mathbb{N}, +, \cdot)$ تصمیم‌ناپذیر است؛

$$\varphi(m, n) \iff \text{الگوریتم شماره } m \text{ در ورودی } n \text{ بایستد}$$

مسئله توقف.

قضیه (هیرونیمی)

فقط دو اثر ضرب به تنهایی موجب تصمیم‌ناپذیری $\mathbb{N}$ می‌شود.

سوال (هیرونیمی)

آیا $(\mathbb{N}, +, <, \lfloor ex \rfloor)$ تصمیم‌پذیر است؟

قضیه (خانی - زارعی - ولی‌زاده)

برای $(\mathbb{N}, +, <, \lfloor \mathsf{e}x \rfloor)$

- *می‌توان یک اصول موضوعه ساده ارائه کرد.*
- *می‌توان بین مدلهای این تئوری بازی کرد.*
- *در نتیجه این تئوری تصمیم‌پذیر است.*

Khani, M., Valizadeh, A. N., and Zarei, A. (2024).
Model-completeness and decidability of the additive structure of integers expanded with a function for a Beatty sequence.
Annals of Pure and Applied Logic, 175(10), 103493.