نتیجه (از کامل بودن ACF_p):

فرمول φ در زبان حلقه‌ها در ساختار $(\mathbb{C}, +, \cdot, 0, 1, -)$

درست است اگر و تنها اگر از جایی به بعد در $\mathbb{F}_p^{alg}$ درست باشد.

$\mathbb{F}_2^{alg} \quad \ldots \quad \mathbb{F}_p^{alg} \quad \ldots \quad \mathbb{F}_q^{alg}$

$\longrightarrow$

مثال

بر نگاشت چندجمله‌ای $F : \mathbb{C}^n \to \mathbb{C}^n$

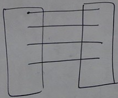
$$F(x_1, \ldots, x_n) = (\underbrace{f_1(x_1, \ldots, x_n)}, \ldots, \underbrace{f_n(x_1, \ldots, x_n)})$$

$$f_i(x_1, \ldots, x_n) \in \mathbb{C}[X_1, \ldots, X_n]$$

اگر یک‌به‌یک باشد، پوشاست.

اثبات

توجه کنید اگر $f : k^n \to k^n$ (k متناهی) اگر یک‌به‌یک باشد آن‌گاه f پوشاست.



فرض کنید F یک لیست چندجمله‌ای از $\mathbb{C}^n$ به $\mathbb{C}^n$ باشد که یک به یک است. فرض کنید که حداکثر درجه‌ی چندجمله‌ای‌های به کار رفته در F برابر با d باشد.

فرمول زیر را در نظر بگیرید:

$\varphi :=$ «هر چندجمله‌ای $F=(f_1(x_1,\dots,x_n),\dots,f_n(x_1,\dots,x_n))$ با حداکثر درجه‌ی d اگر یک به یک باشد پوشاست.»

مثال

هر چندجمله‌ای $f:\mathbb{C}\to\mathbb{C}$ با درجه‌ی 2 اگر یک به یک باشد پوشاست.

$$\forall a_0,a_1,a_2 \left(\left[\forall x,y \ \ a_0+a_1x+a_2x^2=a_0+a_1y+a_2y^2 \to x=y\right] \to \forall t\ \exists t' \ \ a_0+a_1t'+a_2t'^2=t \right)$$

کافی است نشان دهیم که جمله‌ی φ در میدان‌های بسته‌ی جبری با مشخصه‌ی p از جایی به بعد درست است.

یعنی کافی است نشان دهیم که جمله‌ی φ از جایی به بعد در $\mathbb{F}_p^{alg}$ درست است.

اثبات درستی حکم درباره‌ی $\mathbb{F}_p^{alg}$

به برهان خلف فرض کنید حتی جبری F یکی به یک باشد ولی پوشا نباشد.

$(a_1x^2+a_2x^3,\ a_3x^5+a_4x^7)$

$$F: (\mathbb{F}_p^{alg})^n \to (\mathbb{F}_p^{alg})^n$$

$$(x_1,\dots,x_n) \longmapsto (\underbrace{f_1(x_1,\dots,x_n)}_{ax_1x_2+bx_1^2x_3x_4},\dots,f_n(x_1,\dots,x_n))$$

فرض کنید $\bar{a}$ تمام ضرایب موجود باشد. و فرض کنید $\bar{b}$ نقطه‌ای باشد که پیش‌نگاره ندارد.

دقیق کردن این نکته از سمینار خانم داوودی.

$\cdots \subseteq (I) \subseteq \quad \subseteq (III)$

ست همو

$$\mathbb{F}_p^{alg} = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n}$$

هر چند جبری در $\mathbb{F}_{p^n}$ ریشه‌اش در یک میدان متناهی هست

$\mathbb{F}_{p^n}$ قرار می‌گیرد. بنابراین ریشه‌اش در یک $\mathbb{F}_{p^m}$ قرار می‌گیرد.

$$\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}, \quad n<m$$

$$\frac{\mathbb{F}_{p^n}[x]}{\langle f\rangle}$$

Chatzidakis,

MacPherson,

asymptotic sentences...

$$F\restriction \langle \bar{a}, \bar{b}\rangle \to \langle \bar{a}, \bar{b}\rangle$$

یک به یک است.

یعنی تولید شده توسط $\bar{a}, \bar{b}$ که متناهی است.

$$k = \langle \bar{a}, \bar{b}\rangle$$

$$F : k^n \to k^n$$

متناهی

F باید پوشا باشد (تناقض با اینکه F، $\bar{b}$ را نپوشاند).

تصمیم‌پذیری

تعریف

تئوری T را **تصمیم‌پذیر** (decidable) گوییم هرگاه مجموعه $\{\varphi \mid T \models \varphi\}$ بازگشتی باشد؛ به بیان دیگر

الگوریتمی وجود داشته باشد که تعیین کند که برای هر جمله φ آیا $T \models \varphi$ یا $T \not\models \varphi$.

مثال ACF_0 یک تئوری تصمیم‌پذیر است.

$L = \{+, \cdot, 0, 1, -\}$

1. تئوری ACF_0 را می‌توان با الگوریتم تولید کرد.
2. ACF_0 کامل است یعنی برای هر جمله φ یا $ACF_0 \models \varphi$ یا $ACF_0 \models \neg\varphi$.
3. $\underbrace{T \vdash \varphi}_{\text{اثبات برای } \varphi \text{ از } T \text{ وجود داشته باشد}} \iff \underbrace{T \models \varphi}_{\text{در هر مدل } T\text{، } \varphi \text{ درست باشد}}$

$Th(\mathbb{C}) \equiv ACF_0$

$\varphi \in Th(\mathbb{C}) \Leftrightarrow ACF_0 \models \varphi$

مرور

$Th(\mathbb{C}, +, \cdot, 0, 1, -)$

$T = ACF_0$

نتیجه

هر تئوری کامل که با الگوریتم تولید شود

تصمیم پذیر است.

Algorithm:

L

T

$A = \{\varphi \mid T \vdash \varphi\}$

$\varphi \longrightarrow$ الگوریتم $\longrightarrow$

$T \vdash \varphi$: Yes

$T \nvdash \varphi \Rightarrow T \vdash \neg\varphi$

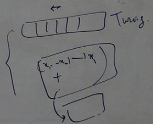
No

<u>سوال</u> آیا برای اعداد طبیعی، یعنی برای ساختار $(\mathbb{N}, +, \cdot)$

$\mathcal{L} = \{+, \cdot\}$

می‌توان یک تئوری کامل الگوریتمی نوشت؟

<u>سوال</u> آیا $Th(\mathbb{N}, +, \cdot)$ تصمیم‌پذیر است؟



<u>تعریف</u>

مجموعهٔ $A \subseteq \mathbb{N}$ را <u>r.e.</u> می‌نامیم (به طور موثر شمارا)

هرگاه <u>الگوریتمی</u> وجود داشته باشد به طوری که برای هر $x \in \mathbb{N}$

اگر $x \in A$ آنگاه الگوریتم بایستد.

مجموعهٔ A را <u>بازگشتی</u> می‌نامیم هرگاه الگوریتمی وجود داشته باشد که تعیین کند آیا $x \in A$ یا $x \notin A$.

پروژه محمد صالحی:

نشان دهید که یک فرمول در زبان $L=\{+,\cdot,1\}$ وجود دارد که عبارت زیر را بیان می‌کند.

$T(e,s,t)$: ماشین تورینگ e ام با ورودی s در زمان t می‌ایستد.

مسئله توقف — Halting problem

هیچ الگوریتمی وجود ندارد که تعیین کند آیا هر الگوریتم x ام با ورودی x می‌ایستد یا خیر.

اثبات: فرض کنیم چنین الگوریتمی وجود داشته باشد.

تابع زیر را در نظر بگیرید:

$$g(x)=\begin{cases} \text{صفر} & \text{اگر الگوریتم } x \text{ ام با ورودی } x \text{ نایستد} \\ \text{loop} & \text{در غیر این صورت} \end{cases}$$

سوال: $g(x)$ خودش یک الگوریتم است.

$\vdots$

$g(x)$: e ام

سوال: آیا الگوریتم e با ورودی e می‌ایستد؟

(Gödel)

قضیهٔ ناتمامیت اول گودل

$Th(\mathbb{N}, +, \cdot, 0, 1)$ تصمیم‌ناپذیر است.

اثبات: فرمول $T(e,s,t)$ وجود دارد که بیانگر آن است

الگوریتم e ام در ورودی s پس از t مرحله می‌ایستد. پس فرمول زیر را در نظر بگیرید.

$$\underbrace{\exists y \quad T(e,s,y)}_{\text{الگوریتم } e \text{ ام با ورودی } s \text{ می‌ایستد}}$$

تمام جملات زیر را در نظر بگیرید

$$\varphi_{e,s}: \exists y \quad T(\underbrace{1+1+\cdots+1}_{e \text{ بار}}, \underbrace{1+1+1+\cdots+1}_{s \text{ بار}}, y)$$

اگر T تصمیم‌پذیر باشد الگوریتمی وجود دارد که تصمیم می‌گیرد که آیا جملات $\varphi_{e,s}$ درست هستند یا خیر و این مسئلهٔ توقف را نقض می‌کند

قضیه ناتمامیت دوم گودل

قضایای درست در مورد اعداد طبیعی وجود دارد که از اصول پئانو نتیجه نمی‌شود.

اصول پئانو: $L = \{+, \cdot, S, 0\}$ (تابع تالی)

$\forall x\ S(x) \neq 0$

$\forall x\ x \neq 0 \to \exists y\ x = S(y)$

$x + 0 = x$

$x + S(y) = S(x+y)$

$x \cdot 0 = 0$

$x \cdot S(y) = x \cdot y + x$

+ اصل استقرا

$\{\varphi(0) \wedge \forall x\ \varphi(x) \to \varphi(S(x)) \to \forall x\ \varphi(x)\}$ ، $\varphi \in$ فرمول L

Jeff-Paris

قضیه ملموس در مورد اعداد طبیعی که از اصول پئانو نتیجه نمی‌شود.

(پاریس - هرینگتون)

ورژن

$x \to (x)^n_k$