پردیس علوم
دانشکده ریاضی، آمار و علوم کامپیوتر

تصمیم‌ناپذیری تألیفی و ناتمامیت گزاره‌های نظام‌های مرتبه اوّل در ابزار Coq

نگارنده

ساجده طالبی

استاد راهنما: دکتر مجتبی مجتهدی

پایان‌نامه برای دریافت درجهٔ کارشناسی
در رشتهٔ علوم کامپیوتر

تاریخ: مرداد ۱۴۰۱

چکیده

زبان Coq، یک زبان تابعی است که در ماشینی کردن برهان‌ها و ساختارهای ریاضی، کاربرد دارد. در این پروژه، با استفاده از رویکرد تألیفی در تصمیم‌ناپذیری، تلاش بر آن است تا تصمیم‌ناپذیری گزاره‌های نظام منطق مرتبه اول اثبات شود. رویکرد تألیفی بر اساس محاسبه‌پذیری همهٔ توابع در پایه‌ای ساختنی مانند نظریهٔ نوع‌های Coq است که بر خلاف نظریهٔ محاسبهٔ کلاسیک که بر مبنای تز چرچ بر روی مدل محاسباتی معینی مانند ماشین تورینگ عمل می‌کند، بدون اتخاذ یك مدل محاسباتی صریح به کار گرفته می‌شود. به طور دقیق‌تر، در این پروژه به دلالت‌های معنایی و قیاسی حساب پئانو (PA) و نظریهٔ مجموعه‌های زرملو-فرانکل (ZF) و تصمیم‌ناپذیری آن‌ها که ناشی از به ترتیب فروکاهش چند به یك حل معادلات دیوفانتی (مانند مسئلهٔ دهم هیلبرت؛ (H_{10})) و مسئلهٔ تناظر پُست (PCP) است، می‌پردازیم. در این رساله نشان می‌دهیم که در رویکرد تألیفی، این فروکاهش‌ها به عنوان توابع سطح متا (meta)، نیازی به کدگذاری در قالب معرفی مدل محاسباتی فرمال و معینی ندارد.
موارد معین PA و ZF، از یک نظریهٔ تألیفی عمومی از گزاره‌های تصمیم‌ناپذیر به دست می‌آید و بر ارتباط بین سازگاری و ناتمامیت تمرکز می‌کند. به طور ویژه، این فروکاهش‌ها بر پایهٔ وجود مدل‌های استانداردی است که فرضیات بیشتری را در ZF و تمام گسترش‌های گزاره‌ای که هنوز با مدل‌های استاندارد توجیه می‌شود، ناتمام نشان داده شده‌اند. نهایتا به عنوان نتیجهٔ جانبی تصمیم‌ناپذیری که با استفاده از تنها عمل عضویت و بدون استفاده از نماد تساوی فرمول‌بندی شده است، تصمیم‌ناپذیری منطق مرتبه اول از تنها یك رابطهٔ دودویی استنتاج می‌شود.

سپاسگزاری

سپاس خدای بزرگ را که مرا یاری رساند تا بتوانم این مقطع تحصیلی را به پایان رسانده و گامی در راستای اعتلای علم بردارم. از استاد راهنمای گرانقدرم جناب آقای دکتر مجتهدی کمال تشکر را دارم که وجودشان همیشه قوتی برای انجام کارهایم بوده است و بدون شک انجام این پایان‌نامه بدون کمک و راهنمایی‌های ارزندهٔ ایشان امکان‌پذیر نبوده است. در پایان به تمامی عزیزانی که در طول انجام این پروژه مرا یاری کرده‌اند، کمال تشکر و قدردانی را ابراز می‌دارم.

پیشگفتار

منطق مرتبه اوّل به عنوان یکی از جریان‌های اصلی فرمالیسم برای زیربنای ریاضیات بوده است که از زمان پیدایش این مدل در اواخر قرن ۱۹ میلادی، از منظرهای مختلف مورد بررسی قرار گرفته است. یکی از جنبه‌های این مدل، جنبهٔ مربوط به ویژگی های الگوریتمی است که با تلاش‌های هیلبرت و آکرمن برای یافتن رویهٔ تصمیم‌گیری برای پاسخ به این پرسش (که تحت عنوان مسئلهٔ *Entscheidungs* از آن یاد می‌شود) آیا فرمول‌های مانند φ وجود دارد که در تمام تعابیر معتبر باشند؟ این فرمول‌ها معمولاً به صورت $\models \varphi$ نوشته می‌شود. تورینگ و چرچ با پژوهش‌های پیشگامانهٔ خود در دههٔ ۱۹۳۰ ثابت کردند که چنین رویهٔ تصمیم‌گیری عموماً نمی‌تواند وجود داشته باشد. با این حال، اگر اعتبار φ را محدود به تعابیری در نظر بگیریم که مجموعه‌ای معین مانند $\mathcal{A}$ را ارضا می‌کنند، این نتیجه تغییر می‌کند. از این دسته از فرمول‌ها به صورت $\mathcal{A} \models \varphi$ استفاده می‌شود.

از سوی دیگر، اگر اصل موضوع $\mathcal{A}$ برای بیان محاسبات به اندازهٔ کافی قوی باشد، تصمیم‌ناپذیری مسئلهٔ یافتن فرمول‌های φ که در $\models \varphi$ صدق کنند، با وجود $\mathcal{A}$ قابل‌اثبات است. در ریاضیات، حساب پئانو (PA) و نظریهٔ مجموعه‌های زرملو-فرانکل (ZF) پایه‌های استاندارد برای شاخه‌های اساسی ریاضیاتند که دقیقاً به دلیل بیانی بودنشان، نمونه‌های بارز این اصول موضوعه هستند.

همانطور که در مبانی سازنده معمول است، تمام توابع قابل تعریف در نظریه نوع Coq هستند به طور موثر قابل محاسبه‌اند؛ بنابراین برای مثال هر تابع بولی روی اعداد طبیعی $f : \mathbb{N} \to \mathbb{B}$ منطبق با یک گزارهٔ $P \subseteq \mathbb{N}$ ممکن است حتی بدون آن ارتباط صریح f به برخی از رمزگذاری‌ها به عنوان ماشین تورینگ، تابع بازگشتی μ، یا بدون تایپ $\lambda - term$ به عنوان یک تصمیم‌گیری برای P درک شود.

در این روش، بسیاری از مفاهیم نظریهٔ محاسبه را می‌توان ارائه کرد که به طور تألیفی، نیاز به یک مدل رسمی متوسط از محاسبات را برطرف کند. علاوه بر این، مفاهیم منفی مانند تصمیم‌ناپذیری عمدتاً با فروکاهش‌ها ارائه می‌شوند، یعنی توابع قابل‌محاسبه که یک مسئله را بر حسب مسئلهٔ دیگر کد می‌کنند. در ابزار Coq برهان تصمیم‌ناپذیری به مسئلهٔ توقف ماشین تورینگ به طور تألیفی فروکاسته می‌شود.

بنابراین، بررسی مجدد تصمیم‌ناپذیری نظام‌های مرتبه اوّل با استفاده از دستیار اثباتی مانند Coq به دلایل متعددی ارزشمند است که با استفاده از رویکرد تألیفی به تصمیم‌ناپذیری باعث ماشینی شدن

نتایج اساسی فراریاضیات می‌شود.
از طرفی می‌دانیم که در مجموعهٔ گزاره‌های تصمیم‌ناپذیر $\mathcal{A}$، این ویژگی وجود دارد که برای فرمول φ هیچ یک از $\mathcal{A} \models \varphi$ و $\mathcal{A} \models \neg\varphi$ به دست نمی‌آید. با استفاده از یکی از نتایج قضیهٔ پُست که بیان می‌کند محمول‌های دوعددی تصمیم‌پذیر هستند، می‌توان $\mathcal{A} \models \varphi$ را با یک نظام قابل شمارش استنتاجی $\mathcal{A} \vdash \varphi$ توصیف می‌کنیم. بنابراین $\mathcal{A} \nvdash \varphi$ را نیز با $\mathcal{A} \vdash \neg\varphi$ توصیف می‌کنیم. بر اساس یک اثبات تألیفی از قضیهٔ پُست، همهٔ گزاره‌های رسالهٔ حاضر به طور تألیفی تصمیم‌ناپذیر نشان داده شده است و ناکامل هستند؛ به این معنا که کامل بودن آنها مستلزم تصمیم‌پذیری تورینگ است. در نهایت، تصمیم‌ناپذیری یک گزارهٔ مرتبه اول $\mathcal{A}$ مانند PA یا ZF را می‌توان تنها در یک نظام قوی‌تر ایجاد کرد، زیرا فروکاهش از یک مسئلهٔ نابدیهی سازگاری $\mathcal{A}$ را نتیجه می‌دهد.

فهرست مطالب

فصل ۱

مفاهیم مقدماتی

۱.۱ نظریهٔ ساختنی نوع

در این رساله در چارچوب یک تئوری نوع سازنده مانند آنچه در Coq پیاده‌سازی شده است، کار می‌کنیم. ارائهٔ یک سلسله مراتب اعتباری از جهان‌های نوع بالاتر از یک جهان منفرد $\mathbb{P}$ از گزاره‌ها در سطح نوع، واحد نوع $\mathbf{1}$ را با یک عنصر واحد داریم $\mathbf{1} : *$، نوع خالی $\mathbf{0}$، فضاهای تابع $X \to Y$، ضرب $X \times Y$، مجموع $X + Y$، ضرب وابسته $\forall(x : X).Fx$ و مجموع وابسته $\Sigma(x : X).Fx$. در سطح گزاره‌ای، این انواع با علامت نشان داده می‌شوند نماد منطقی معمولی ($\bot$، $\top$، $\to$، $\wedge$، $\vee$، $\forall$، و $\exists$). به اصطلاح *حذف بزرگ* از $\mathbb{P}$ به انواع محاسباتی محدود شده است، به ویژه تمایز موارد در اثبات‌های $\vee$ و $\exists$ به شکل مقادیر محاسباتی مجاز نیست. از طرفی این محدودیت به اندازهٔ کافی نفوذپذیر برای حذف زیاد گزارهٔ برابری $=: \forall X.X \to X \to \mathbb{P}$ مشخص‌شده توسط سازندهٔ $\forall(x : X).x = x$، و همچنین تعاریف توابع با بازگشت مناسب است. در این رساله از انواع استقرایی اولیهٔ بولی‌ها ($\mathbb{B} := tt|ff$)، اعداد طبیعی پئانو ($n : \mathbb{N} := 0|n + 1$)، نوع گزینه ($\mathbb{O}(X) := \ulcorner x \urcorner|\emptyset$)، و لیست‌ها ($l : \mathbb{L}(X) := []|x :: l$)، برای طول یک لیست از $|l|$ ، برای الحاق از $l + +\, l'$ و از $x \in l$ برای عضویت استفاده می‌کنیم. و فقط $f[x_1; ...; x_n] := [fx_1; ...; fx_n]$ را برای تابع نگاشت استفاده می‌کنیم. نوع X_n نیز نشانگر بردارهای $\overrightarrow{\forall}$ با طول $n : \mathbb{N}$ بر X است.

۲.۱ تصمیم‌ناپذیری تألیفی

اساس رویکرد تألیفی به نظریهٔ محاسبه، این واقعیت است که همهٔ توابع قابل تعریف در یک پایهٔ ساختنی قابل محاسبه هستند. این واقعیت در مورد بسیاری از انواع آن صدق می‌کند. نظریهٔ ساختنی

نوع اجازه می‌دهد که نوع فرضی در بخش قبل ترسیم شود.
اکنون با مفاهیم مثبت شروع می‌کنیم؛ می‌توانیم تصمیم‌پذیری و شمارش‌پذیری تصمیم را به صورت تألیفی یعنی بدون ارجاع به یک مدل رسمی محاسله، معرفی کنیم:

تعریف ۱.۱. *فرض کنیم $P : X \to \mathbb{P}$ محمولی بر نوع X باشد.*

- *P تصمیم‌پذیر است اگر $f : X \to \mathbb{B}$ وجود داشته باشد که Px اگر و تنها اگر $fx = tt$.*
- *P شمارش‌پذیر است اگر $f : \mathbb{N} \to \mathbb{O}(x)$ وجود داشته باشد که Px اگر و تنها اگر $fn = \ulcorner x \urcorner$ برای $n \in \mathbb{N}$ دلخواه.*

تعریف ۲.۱. *فرض کنیم دو محمول $P : X \to \mathbb{P}$ و $Q : Y \to \mathbb{P}$ داشته باشیم. تابع $f : X \to Y$ را فروکاهش می‌نامیم اگر این شرط برقرار باشد: Px اگر و تنها اگر $Q(fx)$ برای تمام xها. اگر چنین تابعی وجود داشته باشد، می‌نویسیم: $P \preceq Q$.*

گزاره ۳.۱. *اگر $P \preceq Q$ و Q تصمیم‌پذیر باشد آن گاه P نیز تصمیم‌پذیر است.*

چنین فروکاهش هایی قبلاً برای مسئله دهم هیلبرت ((H_{10})) و مسئلهٔ تناظر پست که در رساله حاضر به کار می بریم، تأیید شده است. بنابراین طبق اصل تعدی کافی است تا کاهش مداوم نظام‌های گزاره‌ای در نظر گرفته شده را بررسی کنیم.

۳.۱ نحو، معناشناسی و نظام استنتاجی منطق مرتبه اوّل

در ابتدا با نحو، شروع می‌کنیم، عبارت $t : T$ و فرمول $\varphi : F$ به عنوان انواع استقرایی بر روی نماد ثابت $\Sigma = (\mathcal{F}_\Sigma; \mathcal{P}_\Sigma)$ از نمادهای تابع $f : \mathcal{F}_\Sigma$ و نمادهای رابطه $P : \mathcal{P}_\Sigma$ با تعداد ورودی‌های $|f|$ و $|P|$:

$$t ::= \times_n \quad | \quad f\,\overrightarrow{\mathrm{t}}(n : \mathbb{N}, \overrightarrow{\mathrm{t}} : \mathbb{T}^{|f|})$$

$$\varphi ::= P\,\overrightarrow{\mathrm{t}} \quad | \quad \bot \quad | \quad \varphi \to \psi \quad | \quad \varphi \wedge \psi \quad | \quad \varphi \vee \psi \quad | \quad \forall \varphi \quad | \quad \exists \varphi(t : \mathbb{T}^{|P|})$$

در مرحلهٔ بعد، معناشناسی معمول تارسکی را با ارائهٔ تفسیری از فرمول‌ها تعریف می‌کنیم:

تعریف ۴.۱. *مدل $\mathcal{M}$ از یک دامنه نوع D و همچنین توابع $f^{\mathcal{M}} : D^{|f|} \to D$ و $P^{\mathcal{M}} : D^{|P|} \to \mathbb{P}$ تشکیل شده است نمادها را در نماد Σ تفسیر می‌کند. فرض کنیم یک تابع تخصیص متغیر $\rho : \mathbb{N} \to D$ داشته باشیم، آنگاه ارزیاب هر ترم را به صورت $\hat{\rho} : \mathbb{T} \to D$ و ارضای فرمول $\rho \models \varphi$ را این گونه تعریف می‌کنیم:*

$$\hat{\rho}\times_n := \rho n \qquad \hat{\rho}(f\,\overrightarrow{\mathrm{t}}) := f^{\mathcal{M}}(\hat{\rho}\,\overrightarrow{\mathrm{t}}) \qquad \rho \models P\,\overrightarrow{\mathrm{t}} := P^{\mathcal{M}}(\hat{\rho}\,\overrightarrow{\mathrm{t}})$$

اگر یک مدل $\mathcal{M}$ یک فرمول φ را برای همه تخصیص متغیر ρ برآورده کند، $\mathcal{M} \models \varphi$ می‌نویسیم. علاوه بر این، فرض کنیم یک نظریه $\mathcal{T} : \mathbb{F} \to \mathbb{P}$، داشته باشیم. آنگاه می‌نویسیم $\mathcal{M} \models \mathcal{T}$ اگر $\mathcal{M} \models \psi$ برای همه ψ که $\mathcal{T}\psi$ و می‌نویسیم $\mathcal{T} \models \varphi$ اگر $\mathcal{M} \models \mathcal{T}$ به ازای هر $\mathcal{M}$ نتیجه دهد $\mathcal{M} \models \varphi$. به طریق مشابه، این تعاریف برای فضای متناهی $\Gamma : \mathbb{L}(\mathbb{F})$ نیز صادق است.
در نهایت، نظام‌های استنتاجی را به عنوان محمولات استقرایی از نوع $\mathbb{L}(\mathbb{F}) \to \mathbb{F} \to \mathbb{P}$ نشان می‌دهیم. در این رساله، استنتاج طبیعی شهودی و کلاسیک $\Gamma\vdash_i\varphi$ و $\Gamma\vdash_c\varphi$ را در نظر می‌گیریم، به ترتیب، و اگر عبارتی برای هر دو گونه اعمال می‌شود، $\Gamma\vdash\varphi$می‌نویسیم.

$$\frac{\Gamma[\uparrow] \vdash \varphi}{\Gamma \vdash \forall\varphi} AI \quad \frac{\Gamma \vdash \forall\varphi}{\Gamma \vdash \varphi[t]} AE \quad \frac{\Gamma \vdash \varphi[t]}{\Gamma \vdash \exists\varphi} EI \quad \frac{\Gamma \vdash \exists\varphi \quad \Gamma[\uparrow], \varphi \vdash \psi[\uparrow]}{\Gamma \vdash \psi} EE$$

که برای منطق شهودگرایانه داریم:

$$\frac{\Gamma \vdash \varphi[\times_n]}{\Gamma \vdash \forall\varphi} \times_n \notin \Gamma, \varphi.AI \quad \frac{\Gamma \vdash \exists\varphi \quad \Gamma, \varphi[\times_n] \vdash \psi}{\Gamma \vdash \psi} \times_n \notin \Gamma, \varphi, \psi.EE$$

فصل ۲

نظام‌های گزاره‌ای تصمیم‌ناپذیر و ناکامل مرتبه اوّل

در این بخش، برخی از جنبه‌های الگوریتمی کلی در مورد گزاره‌های مرتبه اول را بررسی می‌کنیم و طرح مشترکی را که در زمینهٔ شواهد تصمیم‌ناپذیری ارائه شده ترسیم می‌کنیم. سپس یک اثر قابل شمارش و گسسته Σ را ثابت می‌کنیم.

تعریف ۱.۲. *تئوری* $\mathcal{A} : \mathbb{F} \to \mathbb{P}$ *یک* ***گزاره‌سازی*** *است اگر* $\mathcal{A}$ *شمارش‌پذیر باشد.*

هر گزاره‌سازی داده‌شده باعث ایجاد دو مسئلهٔ تصمیم‌پذیری مرتبط می‌شود؛ یعنی دلالت معنایی $\mathcal{A} \models := \lambda\varphi.\mathcal{A} \models \varphi$ و التزام استنتاجی $\mathcal{A} \vdash := \lambda\varphi.\mathcal{A} \vdash \varphi$. از آنجایی که ساختار ما نشان می‌دهد که نظام استنتاجی کلاسیک $\vdash_c$ نه درست است و نه کامل، ما عمدتاً یک مفهوم ترکیبی از معناشناسی کلاسیک و استنتاج شهودی را در نظر می‌گیریم:

تعریف ۲.۲. *گوییم محمول* $P : X \to \mathbb{P}$ *به* $\mathcal{A}$ *فروکاسته می‌شود و به صورت* $P \preceq \mathcal{A}$ *نمایش داده می‌شود اگر تابعی مانند* $f : X \to \mathbb{F}$ *وجود داشته باشد که* $P \preceq \mathcal{A}^{\models}$ *و* $P \preceq \mathcal{A}^{\vdash}$ *را ارضا کند.*

با فرض قانون میانی مستثنی $LEM := \forall p : \mathbb{P}.p \vee \neg p$ برای به دست آوردن $P \preceq \mathcal{A}^{\vdash_c}$ از $P \preceq \mathcal{A}^{\models}$ کافی است؛ چون همزمان داریم: $\mathcal{A} \vdash_c \varphi$ و $\mathcal{A} \models \varphi$. در واقع، در حال حاضر درستی گزاره‌ها برای مطالعات موردی ما در مورد PA و ZF کافی است؛ زیرا می‌دانیم با داشتن Px، رسیدن به $\mathcal{A} \vdash fx$ بدون نیاز به تمامیت امکان‌پذیر است.

گزاره ۳.۲. *اگر* $P \preceq \mathcal{A}^{\vdash}$ *و وجود داشته باشد* x *که* $\neg Px$ *آن‌گاه* $\mathcal{A} \nvdash \bot$.

اثبات. اگر $f : X \to \mathbb{F}$ شاهدی بر $P \preceq \mathcal{A}^{\vdash}$ باشد، آنگاه با $\neg Px$ به $\mathcal{A} \nvdash fx$ می‌رسیم. حال با قواعد نظام استنتاجی می‌توان $\mathcal{A} \nvdash \bot$ را از آن استنتاج کرد. □

تعریف ۴.۲. *$\mathcal{A}$ کامل است اگر برای هر φ بسته، یکی از $\mathcal{A} \vdash_c \varphi$ یا $\mathcal{A} \vdash_c \neg\varphi$ را داشته باشیم.*

گزاره ۵.۲. *اگر $\mathcal{A}$ با $\mathcal{A} \vdash_c \neg\varphi$ کامل باشد، آنگاه $\lambda\varphi.\mathcal{A} \vdash_c \varphi$ برای φ بسته، تصمیم‌گیرنده است. در نتیجه، اگر f شاهدی بر $P \preceq \mathcal{A}^{\vdash_c}$ به طوری که برای تمام fx ها بسته باشد، آنگاه P تصمیم‌پذیر است.*

اثبات. با نسخهٔ تألیفی قضیهٔ پُست، می‌توان نشان داد که $\mathcal{A} \vdash_c$ دوعددی است؛ یعنی هم $\lambda\varphi.\mathcal{A} \vdash_c \varphi$ شمارش‌پذیر است و هم $\lambda\varphi.\mathcal{A} \nvdash_c \varphi$ و به طور منطقی تصمیم‌پذیرند. این به این معناست که برای هر φ یکی از $\mathcal{A} \vdash_c \varphi$ یا $\mathcal{A} \nvdash_c \varphi$ برقرار است. بنابراین، $\vdash_c$ شمارش‌پذیر است و چون سازگار و کامل نیز هست، $\mathcal{A} \nvdash_c \varphi$ اگر و تنها اگر $\mathcal{A} \vdash_c \neg\varphi$. حال طبق قضیهٔ ۳.۱، حکم ثابت می‌شود. □

قضیه ۶.۲. *مسئلهٔ $P : X \to \mathbb{P}$، اصل موضوعی $\mathcal{A}$، مفهوم استاندارد بودن در مدل‌های $M \models \mathcal{A}$ و تابع $\mathcal{F} \ni \_ : X \to$ را با ویژگی های زیر را در نظر بگیرید:*

(i) $\mathcal{A} \models \varphi_x$ بر Px دلالت دارد.

(ii) هر مدل استاندارد $M \models \mathcal{A}$ با $M \models \varphi_x$ را نتیجه می‌دهد.

(iii) $\mathcal{A} \vdash \varphi_x$ بر Px دلالت دارد.

آنگاه $P \preceq \mathcal{B}$ برای همهٔ $\mathcal{B} \supseteq \mathcal{A}$ که یک مدل استاندارد را می‌پذیرد. همچنین با در نظر گرفتن LEM آنگاه $P \preceq \mathcal{B}^{\vdash_c}$.

اثبات. با اثبات $P \preceq \mathcal{B}^{\models}$ شروع می‌کنیم. اینکه $\mathcal{B} \models \varphi_x$ بر Px دلالت دارد به صورت مستقیم از (i) حاصل می‌شود، زیرا هر مدلی از $\mathcal{B}$ مدلی از $\mathcal{A}$ است. متقابلاً، اگر $\mathcal{B} \models \varphi_x$ آنگاه مدل استاندارد مفروض $M \models \mathcal{B}$ نیز φ_x را برآورده می‌کند. بنابراین Px را با (ii) به دست می‌آوریم.
اثبات جهت اول $P \preceq \mathcal{B}^{\vdash_c}$ با فروکاهش ویژگی (iii) بدیهی است. برای جهت دیگر، در نظر می‌گیریم $\mathcal{B} \vdash \varphi_x$ در نتیجه $\mathcal{B} \models \varphi_x$ و به این ترتیب Px را با استدلال قبلی با تکیه بر (ii) نتیجه می‌گیریم.
در نهایت با فرض LEM $P \preceq \mathcal{B}^{\vdash_c}$ را نتیجه می‌گیریم. □

البته (i) از (iii) به وسیله تمامیت حاصل می‌شود، بنابراین تأیید معنایی اولیه و استراتژی غیررسمی که قبلاً ذکر شد، را می‌توان از قضیه حذف کرد. با این حال، ترجیح می‌دهیم که ابتدا یک تأیید معنایی مستقل را بدون سربار معرفی‌شده با کار در یک سیستم استنتاج نحوی، که عمدتاً در مکانیزاسیون Coq آشکار می‌شود، ارائه کنیم. همچنین توجه داشته باشید که نیاز به یک مدل استاندارد هیچ باری در PA نخواهد داشت، اما در مورد ZF این نیاز به تجزیه و تحلیل دقیق پیش‌شرط‌ها دارد.

این بخش را با این گزارهٔ مهم به پایان می‌رسانیم که می‌توانیم مسئلهٔ تصمیم‌گیری برای گزاره‌سازی متناهی A را به مسئلهٔ کلاسیک Entscheidung از منطق مرتبه اول در مورد اعتبار و اثبات‌پذیری در یک بافت تهی فرور بکاهیم.

گزاره ۷.۲. *برای همهٔ* $A : \mathbb{L}(\mathbb{F})$ *داریم* $A^{\vDash} \preceq (\lambda\varphi.\, \vDash \varphi)$ *و* $A^{\vdash} \preceq (\lambda\varphi.\, \vdash \varphi)$.

اثبات. اثبات اینکه تابع $\lambda\varphi.\, \wedge A \to \varphi$ با پیشوندی φ با عطف همهٔ فرمول‌های A هر دو فروکاهش را ایجاد می‌کند، واضح است. □

فصل ۳

حساب پئانو

ما با یک مطالعه موردی نسبتاً ساده شروع می‌کنیم تا رویکرد کلی خود را نسبت به تصمیم‌ناپذیری و ناتمامیت نشان دهیم. برای تئوری حساب پئانو (PA) ما از یک امضا حاوی نمادهایی برای ثابت صفر، تابع جانشین، جمع، ضرب و برابری استفاده می کنیم:

$$(O, S\_\_, \_\_ \oplus \_\_, \_\_ \otimes \_\_; \_\_ \equiv \_\_)$$

هستهٔ PA شامل اصول متعارفی است که جمع و ضرب را مشخص می‌کند:

$$\oplus - base : \forall x.O \oplus x \equiv x \qquad \oplus - recursion : \forall xy.(Sx) \oplus y \equiv S(s \oplus y)$$
$$\otimes - base : \forall x.O \otimes x \equiv O \qquad \otimes - recursion : \forall xy.(Sx) \oplus y \equiv y \oplus x \otimes y$$

لیست Q' متشکل از این چهار اصل برای تصممی‌ناپذیری به اندازهٔ کافی قدرتمند است. تصمیم‌ناپذیری (و ناتمامیت) سپس به طور ویژه به اصل (بی‌نهایت) PA تبدیل می‌شود. با اضافه کردن

$$Disjointness : \forall x.Sx \equiv O \to \bot \qquad Injectivity : \forall xy.Sx \equiv Sy \to x \equiv y$$

و طرح بدیهی استقرا [1] ، که ما آن را به عنوان یک تابع نظری نوع در فرمول‌ها تعریف می‌کنیم:
$\lambda\varphi.\varphi[O] \to (\forall x.\varphi[x] \to \varphi[Sx]) \to \forall x.\varphi[x]$
یکی دیگر از مراجع در زمینه ناتمامیت، محاسبات رابینسون Q است که با جایگزین کردن طرح استقرایی با اصل $\forall x \equiv O \vee \exists y.x \equiv Sy$ به دست می‌آید. مسئلهٔ دهم هیلبرت (H_{10}) به حل‌پذیری معادلات دیوفانتی [2] مربوط می‌شود و به عنوان یک مسئلهٔ طبیعی برای نشان دادن تصمیم‌ناپذیری PA مطرح می‌شود، زیرا معادلات یک قطعهٔ نحوی از فرمول‌های PA هستند. به

[1] axiom scheme of induction
[2] Diophantine equation

طور دقیق‌تر، H_{10} شامل تصمیم‌گیری این است که آیا معادلهٔ دیوفانتی $p = q$ دارای جوابی در اعداد طبیعی $\mathbb{N}$ است، که در آن p و q چند جمله‌ای‌هایی هستند که توسط پارامترها، متغیرها، جمع و ضرب ساخته می‌شوند:

$$\text{p, q} ::= \text{a}_n \mid \text{var } k \mid \text{add p q} \mid \text{mult p q} \qquad (n, k : \mathbb{N})$$

ارزیابی $[\![p]\!]_\alpha$ برای چندجمله‌ای p برای تخصیص متغیر $\alpha : \mathbb{N} \to \mathbb{N}$ به صورت زیر تعریف می‌شود.

$$[\![\text{a}]\!]_\alpha := n \quad [\![\text{var } k]\!]_\alpha := \alpha k \quad [\![\text{add } p\ q]\!]_\alpha := [\![p]\!]_\alpha + [\![q]\!]_\alpha$$

$$[\![\text{mult } p\ q]\!]_\alpha := [\![p]\!]_\alpha \times [\![q]\!]_\alpha$$

تعریف ۱.۳. *$v : \mathbb{N} \to \mathbb{T}$ را به صورت بازگشتی با $v(0) := O$ و $v(n+1) := S(v(n))$ تعریف می‌کنیم. سپس با تعریف $p^* : \mathbb{T}$ چندجمله‌ای‌ها را به صورت بازگشتی به PA ترجمه می‌کنیم:*

$$a_n^* := (n) \quad (var\ k)^* := x_k \quad (add\ p\ q)^* := p^* \oplus q^* \quad (mult\ p\ q)^* := p^* \otimes q^*$$

به این ترتیب می‌توان یک معادلهٔ دیوفانتی از درجهٔ N به فرم $\varphi_{p,q} := \exists^N p^* \equiv q^*$ تبدیل کرد. در این فرمول از N به عنوان سور وجودی برای درونی کردن شرایط حل‌پذیری استفاده می‌کنیم. در نتیجه، فرمول $\varphi_{p,q}$ وجود یک جواب برای $p = q$ را اثبات می‌کند که این تبدیلی از معادلات دیوفانتی به PA را به ما می‌دهد.

لم ۲.۳. *اگر $\exists^N \varphi$ بسته باشد، آنگاه:*

(i) $\mathcal{M} \models \exists^N \varphi$ اگر و تنها اگر $\rho : \mathbb{N} \to \mathcal{M}$ وجود داشته باشد به طوری که $\rho \models \varphi$.

(ii) $\Gamma \vdash \exists^N \varphi$ اگر و تنها اگر $\sigma : \mathbb{N} \to \mathbb{T}$ وجود داشته باشد به طوری که $\Gamma \vdash \varphi[\sigma]$.

اثبات. در این قسمت فقط مقداری شهود برای (i) ارائه می‌دهیم. با فرض $\mathcal{M} \models \exists^N \varphi$ گزاره $\forall \rho . x_1, ..., x_N : \mathcal{M} : \rho \models \varphi$ حاصل می‌شود به طوری که $x_1, ..., x_N$ در نتیجه به طور مشخص برای $\rho' := x_1; ...; x_N; (\lambda x . O^{\mathcal{M}})$ داریم $\rho' \models \varphi$ که درستی ادعایمان را نشان می‌دهد. برای سمت دیگر ρ را با $\rho \models \varphi$ داریم. اگر قرار دهیم $\varphi' := x_1; ...; x_N; (\lambda x . \rho(x + N)$ داریم $\rho = \rho(0); ...; \rho(N); \rho'$ و در نتیجه $x_1, ..., x_N : \mathcal{M}$ وجود دارند که $\rho' \models \varphi$: $x_1, ..., x_N$. چون φ حداکثر N متغیر آزاد دارد، ρ' می‌تواند به هر $\tau : \mathbb{N} \to \mathcal{M}$ تغییر یابد. □

با لم ۲.۳ نشان دادیم، $\varphi_{p,q}$ معادل یافتن یک محیط اثبات‌پذیر $\rho : \mathbb{N} \to \mathcal{M}$ برای $p^* \equiv q^*$ در مدل $\mathcal{M}$ یا به صورت استنتاجی نشان می‌دهد که جایگزینی $\sigma : \mathbb{N} \to \mathbb{T}$ آن را حل می‌کند. این ما را قادر می سازد تا یک راه حل برای $p = q$ را به مدل و سیستم استنتاجی انتقال دهیم.
اکنون بخش معنایی کاهش را برای قطعه اصلی Q' تأیید می‌کنیم. برای این منظور، یک مدل $M \models Q'$ را برای تعاریف و لم‌های بعدی در نظر می‌گیریم.

تعریف ۳.۳. *ما* $\mu : \mathbb{N} \to \mathcal{M}$ *را با* $\mu(0) := O^{\mathcal{M}}$ *و* $\mu(n+1) := S^{\mathcal{M}}(\mu(n))$ *تعریف می‌کنیم.*

اصول موضوعی در Q' برای اثبات هم‌ریختی μ کافی است.

لم ۴.۳. *برای* $n, m : \mathbb{N}$ ، $\mu(n+m) = \mu(n) \oplus^{\mathcal{M}} \mu(m)$ *و* $\mu(n+m) = \mu(n) \otimes^{\mathcal{M}} \mu(m)$.

اثبات. اثبات جمع با استقرا بر روی $n : \mathbb{N}$ و با استفاده از اصول موضوعه جمع در Q انجام می‌شود. اثبات ضرب نیز به همین صورت انجام می‌شود، با استفاده از اصول موضوعه برای ضرب و نتیجه قبلی برای جمع. □

لم ۵.۳. *برای هر* $\rho : \mathbb{N} \to \mathcal{M}$ *و* $n : \mathbb{N}$ *داریم* $\hat{\rho}(v(n)) = \mu(n)$.

با توجه به تخصیص $\alpha : \mathbb{N} \to \mathbb{N}$ ، می‌توانیم ارزیابی یک چندجمله‌ای $[\![p]\!]_\alpha$ را با اعمال μ به هر مدل Q' انتقال دهیم. ویژگی یک‌ریختی μ اکنون تأیید اینکه ما با ارزیابی نسخه تبدیل‌شده p^* با ترکیب $\mu \circ \alpha$ به همان نتیجه می‌رسیم را آسان می‌کند.

لم ۶.۳. *برای هر چندجمله‌ای* p *و* $\alpha : \mathcal{N} \to \mathcal{N}$ *داریم* $\widehat{\mu \circ \alpha}(p^*) = \mu([\![p]\!]_\alpha)$.

اثبات. با استقرا روی p و استفاده از لم‌های ۵.۳ و ۶.۳. □

نتیجه ۷.۳. *اگر* $p = q$ *دارای جواب* α *باشد، آنگاه در هر مدل* Q' ، $(\mu \circ \alpha) \models p^* \equiv q^*$

اثبات. داریم

$$\mu([\![p]\!]_\alpha) = \mu([\![q]\!]_\alpha) \xrightarrow{۶.۳} \widehat{(\mu \circ \alpha)}(p^*) = \widehat{(\mu \circ \alpha)}(q^*) \Rightarrow (\mu \circ \alpha) \models p^* \equiv q^*$$ □

گزاره ۸.۳. *اگر* $p = q$ *پاسخی داشته باشد، آنگاه* $Q' \models \varphi_{p,q}$

اثبات. فرض کنید α جواب $p = q$ است، آنگاه طبق نتیجه ۷.۳ $(\mu \circ \alpha) \models p^* \equiv q^*$ و چون $\exists^N p^* \equiv q^*$ طبق فرض بسته است، نتیجه دلخواه از لم ۲.۳ حاصل می‌شود. □

با توجه به جهت معکوس، انتخاب طبیعی برای یک مدل استاندارد، نوع $\mathbb{N}$ است.

لم ۹.۳. $\mathbb{N}$ *مدلی برای* Q' ، Q *و* PA *است.*

اگر $\mathbb{N} \models \varphi_{p,q}$ باشد، به دست آوردن جواب معادله $p = q$ آسان است.

گزاره ۱۰.۳. *اگر* $\mathbb{N} \models \varphi_{p,q}$ *آنگاه* $p = q$ *جواب دارد.*

اثبات. طبق فرض داریم $\mathbb{N} \models \varphi_{p,q}$ ،پس با استفاده از لم ۲.۳ $\alpha : \mathcal{N} \to \mathcal{N}$ به دست می‌آید که
$\alpha \models p^* \equiv q^* \Rightarrow \widehat{(\mu \circ \alpha)}(p^*) = \widehat{(\mu \circ \alpha)}(q^*) \underrightarrow{۶.۳} \mu([\![p]\!]_\alpha) = \mu([\![q]\!]_\alpha)$
ار آنجا که تابع μ روی $\mathbb{N}$ به سادگی همانی است، می‌توان اضافه کرد که $[\![p]\!]_\alpha = [\![q]\!]_\alpha$ □

بخش استنتاجی کاهش را می توان به طور مشابه به گزاره ۸.۳ نشان داد، و اثبات تمام نتایج میانی را به عنوان مشتقات ND بیان می‌شود. ما فقط عبارات مربوطه را لیست می کنیم و برای جزئیات بیشتر به کد Coq مراجعه می‌کنیم.

لم ۱۱.۳. *برای* $n, m : \mathbb{N}$ *داریم* $Q' \vdash v(n+m) \equiv v(n) \oplus v(m)$ و $Q' \vdash v(n \times m) \equiv v(n) \otimes v(m)$

لم ۱۲.۳. *اگر* α *پاسخی برای* $p = q$ *باشد، آنگاه می‌توان استنباط کرد* $Q' \vdash (p^* \equiv q^*)[v \circ \alpha]$.

گزاره ۱۳.۳. *اگر* $p = q$ *پاسخی داشته باشد، آنگاه* $Q' \vdash \varphi_{p,q}$.

اکنون همه گزاره‌ها را برای بررسی فروکاهش قضیه ۶.۲ در اختیار داریم.

قضیه ۱۴.۳. $H_{10} \preceq Q'$ ، $H_{10} \preceq Q$ و $H_{10} \preceq PA$.

اثبات. از آنجایی که $\mathbb{N}$ یک مدل استاندارد برای Q' ، Q و PA است، ادعاها از قضیه ۶.۲ پیروی می‌کنند زیرا ما سه شرط لازم را در گزاره‌های ۸.۳ ، ۱۰.۳ و ۱۳.۳ نشان داده ایم. □

در نتیجه این فروکاهش‌ها، می‌توان ناتمامیت را به صورت زیر نتیجه گرفت:

قضیه ۱۵.۳. *با فرض* LEM ، *کامل بودن هر پسوند* $\mathcal{A} \supseteq Q'$ *که توسط مدل استاندارد* $\mathbb{N}$ *برآورده شده است، مستلزم تصمیم‌پذیری مساله توقف* [۳] *در ماشین‌های تورینگ است.*

اثبات. به کمک قضایای ۶.۲ و ۱۴.۳ و گزاره ۵.۲ ثابت می‌گردد. □

ما این بخش را با یک نکته در مورد جداسازی مدل‌های Q' ، Q و PA می‌بندیم. برای هر $n : \mathbb{N}$ ، ضریب $\mathbb{Z}/n\mathbb{Z}$ مدلی از Q است. بنابراین به طور خاص Q' مدل بی اهمیت را می‌پذیرد و بنابراین می‌تواند با $\forall xy.x \equiv y$ تکمیل شود، که این موضوع آن را از Q و PA جدا می‌کند، زیرا آنها فقط مدل‌های بی‌نهایت را می‌پذیرند و اساساً ناقص هستند. یک مدل معروف که Q و PA را از هم جدا می‌کند با گسترش $\mathbb{N}$ به $\mathbb{N}^\infty$ با حداکثر عدد ∞ به دست می‌آید.

[3] halting problem

فصل ۴

نظریهٔ مجموعه‌های ZF با توابع اسکولِم

با عطف به نظریه مجموعه‌ها، ابتدا دربارهٔ یک نماد غنی مطالعه می‌کنیم که نمادهای تابع را برای گزاره‌سازی ZF ارائه می‌کند. برای آن نماد داریم:

$$\Sigma := (\emptyset, \{\_\_, \_\_\}, \cup\_\_, \mathcal{P}(\_\_), \omega; \_\_ \equiv \_\_, \_\_ \in \_\_)$$

با استفاده از توابع اسکولِم برای گزاره‌سازی و سایر عملیات قابل تعریف، معمولاً در نظریهٔ مجموعه‌ها، ادبیات و تعریف و تأیید فروکاهش تصمیم‌ناپذیری کار ما را آسان می‌کند. نکتهٔ مهم در این جا، نمایش طرح های گزاره به عنوان توابع $\mathbb{F} \to \mathbb{F}$ است؛ برای مثال طرح جداسازی را به این صورت بیان می‌کنیم:

$$\lambda\varphi.\forall x.\exists y.\forall z.z \in y \longleftrightarrow z \in x \wedge \varphi[x]$$

پس از طرح کلی برای اثبات تصمیم‌ناپذیری در این رساله، ابتدا بر روی تأیید کاهش به نظریه پایه Z' و سپس گسترش به گزاره‌های قوی‌تر با استفاده از قضیه ۶.۲ تمرکز می‌کنیم. به عنوان یک مسئلهٔ اولیه برای این فروکاهش، به طور طبیعی می‌توانیم هر کدام را انتخاب کنیم. مسئلهٔ تصمیم‌گیری از آنجایی که نظریهٔ مجموعه‌ها یک پایهٔ هدف کلی است که بیان خوبی برای اکثر انواع ریاضیات استاندارد است. با این حال، انتخاب دقیق بر فرآیندمان تأثیرگذار است؛ چراکه، فرمال کردن مسئلهٔ توقف ماشین تورینگ در نوع Coq به اندازهٔ کافی دشوار است. بنابراین ما کاهش خود را به Z بر اساس مسئله قضیهٔ پست (PCP) که دارای خصوصیات استقرایی ساده است که یک مسئله تطبیق را با توجه به پشته S محدود بیان می‌کند. جفت (s, t) رشته‌های بولی:

$$\frac{(s,t) \in S}{S \triangleright (s,t)} \qquad \frac{S \triangleright (u,v) \quad (s,t) \in S}{S \triangleright (su, tv)} \qquad \frac{S \triangleright (s,s)}{PCP\ \ S}$$

به طور غیررسمی، S برای استخراج جفت‌های (s,t) استفاده می‌شود که $S \triangleright (s,t)$ با اضافه کردن مکرر جفت ها از مؤلفهٔ پشته به هر ترتیب یا تعداد زیادی نوشته می‌شود. این مثال S یک راه حل را می‌پذیرد و آن را به صورت PCP S بیان می‌کند، اگر یک جفت تطبیق (s،s) را بتوان با این روش مشتق کرد.
رمزگذاری داده‌هایی مانند اعداد و بولی‌ها در شرایط نظریهٔ مجموعه‌ها استاندارد است. با استفاده از نمادهای مشتق‌شدهٔ معمول برای اجتماع دوتایی $x \cup y$، مجموعهٔ تک‌عضوی x و جفت مرتب (x,y) داریم:

$$i : \bar{0} := \emptyset \ \ and \ \ \overline{n+1} := \bar{n} \cup \{\bar{n}\} \qquad ii : \overline{b_1, ..., b_n} := (\bar{b_1}, (...(\bar{b_n}, 0)))$$
$$iii : \overline{tt} := \{\emptyset\} \ \ and \ \ \overline{ff} := \emptyset \qquad iv : \bar{S} := \{(\bar{s_1}, \bar{t_1}), ..., (\bar{s_n}, \bar{t_n})\}$$

که i برای اعداد، ii برای رشته‌ها، iii برای بولی‌ها و iv برای استک‌هاست.
با شروع با یک ایده غیرفرمال، شرایط حل‌پذیری PCP را می‌توان به طور مستقیم بیان کرد؛ در نظریهٔ مجموعه‌ها فقط با اثبات وجود مجموعه‌ای که مطابقت را برای S کد می‌کند:

$$\exists x.(x,x) \in \bigcup_{k \in \omega} \bar{S}^k \ \ where \ \ \bar{S}^0 = \bar{S} \ \ and \ \ \bar{S}^{k+1} = S \boxtimes \bar{S}^k =$$
$$\bigcup_{s/t \in S} \{(\bar{s}x, \bar{t}y) | (x,y) \in \bar{S}^k\}$$

ساختار اصلی مورد استفاده در قضیه بازگشتی برای ω، دنباله‌ای متناهی از تقریب f جمع‌آوری اولین k گام معادلات بازگشتی است. از آنجایی که در مورد ما نیازی نیست که حد دنباله‌هایی را تشکیل دهیم که به تقریب‌ها برای توافق نیاز دارد، برای اطمینان از اینکه حداقل k گام اول بدون قطع شدن، یعنی محدود شده‌اند، کافی است. داریم:

$$f \gg k := (\emptyset, \bar{S}) \in f \wedge \forall (l,B) \in f.l \in k \rightarrow (l \cup \{l\}, S \boxtimes B) \in f$$

که ما از عملیات $S \boxtimes B$ استفادهٔ مجدد می‌کنیم و عناصر کدگذاری‌شده لیست S را به صورت جزء به عناصر مجموعه B همانطور که در بالا مشخص شده است اضافه می‌کنیم. توجه داشته باشید که این عملیات واقعا قابل تعریف به عنوان یک تابع $\mathbb{L}(\mathbb{B}) \rightarrow \mathbb{T} \rightarrow \mathbb{T}$ نیست و باید با کمی کردن آن را دور زد. با این حال، ما این ظرافت را به کد Coq واگذار می کنیم و به استفاده از $S \boxtimes B$ به عنوان یک تابع ادامه می‌دهیم.
اکنون حل‌پذیری S را می‌توان به‌طور فرمال به صورت وجود تقریب تابعی f به طول k که حاوی یک زوج (x,x) است بیان کرد:

$$\varphi s := \exists k, f, B, x.k \in \omega \wedge (\forall (l,B), (l,B') \in f.B = B') \wedge f \gg k$$
$$\wedge (k,B) \in f \wedge (x,x) \in B$$

لم ۱.۴. *فرض کنیم* $n, m : \mathbb{N}$ *و* $s, t : \mathbb{L}(\mathbb{B})$ *را داریم. آنگاه خواهیم داشت:*

(i) $\mathcal{M} \models \bar{n} \in \omega$	***(iii)*** $\mathcal{M} \models \bar{n} \equiv \bar{m}\ \ implies\ \ n = m$
(ii) $\mathcal{M} \models \bar{n} \notin \bar{n}$	***(iv)*** $\mathcal{M} \models \bar{s} \equiv \bar{t}\ \ implies\ \ s = t$

اثبات. (i) با استقرا روی n، با استفاده از اصل بی نهایت که ω را مشخص می‌کند.
(ii) مجدداً با استقرا بر روی n، با استفاده از این واقعیت که اعداد n مجموعه‌های متعدی هستند.
(iii) با اصل تثلیث داریم $n < m$ یا $n = m$ یا $m < n$. اگر $n < m$ بود، سپس $\mathcal{M} \models \bar{n} \in \bar{m}$ با استقرای ساختی دنبال می‌شود. ولی سپس فرض $\mathcal{M} \models \bar{n} \equiv \bar{m}$ به $\mathcal{M} \models \bar{n} \in \bar{n}$ را در تضاد با (ii) به دست می‌دهد.
(iv) با استقرا در رشته‌های داده شده، با استفاده از تزریق رمزگذاری بولی به دست می‌آید. □

به منظور مطابقت با ساختار مشتقات تکرارشده کدگذاری شده در φ_S، لازم است مجددا فرمول‌بندی $S \triangleright (s, t)$ را انجام دهیم با مراجعه به مشتقات ترکیبی S^n به طول n که اکنون با مراجعه به بازگشت روی $n : \mathbb{N}$ از طریق $S^0 := S$ و $S^{n+1} := S \boxtimes S^n$ با استفاده مجدد از عملیات $\boxtimes$ برای لیست‌ها انجام می‌شود.

لم ۲.۴. $S \triangleright (s, t)$ *اگر و تنها اگر وجود داشته باشد* $n : \mathbb{N}$ *که* $(s, t) \in S^n$.

سپس تکرارهای S^n را می‌توان به عنوان توابع سطح مجموعه $f_n^S := \{(\emptyset, \bar{S}), ..., (\bar{n}, \bar{S^n})\}$ کدگذاری کرد که در واقع توسط مدل $\mathcal{M}$ به عنوان تقریب صحیح شناخته می شوند:

لم ۳.۴. *برای هر* $n : \mathbb{N}$ *داریم* $\mathcal{M} \models f_n^S \gg \bar{n}$.

اثبات. در این اثبات ما در $\mathcal{M}$ کار می‌کنیم تا عبارات میانی را ساده کنیم. برای اولین پیوند، باید نشان دهیم که $(\emptyset, \bar{S}) \in {f_S}^n$ که ساده است زیرا $(\emptyset, \bar{S}) \in {f_S}^0$ و ${f_S}^m \subseteq {f_S}^n$ هر زمان که $m \leq n$. در مورد پیوند دوم، فرض می‌کنیم $(k, B) \in {f_S}^n$ و هم‌چنین $k \in \bar{n}$ و باید نشان دهیم $(k \cup \{k\} S \boxtimes B) \in {f_S}^n$. از $(k, B) \in {f_S}^n$ بدست می‌آوریم که وجود دارد m با $k = \bar{m}$ و $B = \overline{S^m}$ است. سپس از $m \in n$ و از این رو $m < n$ و نیز استنباط می‌کنیم $(\overline{m+1}\overline{S^{m+1}}) f S n$. این ادعا از آنجایی که $m + 1 = k \cup \{k\}$ و $S \boxtimes B = S \boxtimes \overline{S^n} = \overline{S \boxtimes S^n} = \overline{S^{m+1}}$ با استفاده از اینکه عملیات $\boxtimes$ در لیست ها به ترتیب مجموعه ها به خوبی با رمزگذاری رشته‌ها تعامل دارد به دست می‌آید. □

گزاره ۴.۴. *اگر* S *آنگاه* PCP $Z' \models \varphi_S$.

اثبات. با فرض PCP S، $s : \mathcal{L}(\mathcal{B})$ و $n : \mathbb{N}$ با $(ss) \in S^n$ با استفاده از لم ۲.۴ وجود دارد. برای اثبات $Z' \models \varphi_S$ فرض می‌کنیم $\mathcal{M} \models Z'$ و باید $Z' \models \varphi_S$ را نشان دهیم. نمونه‌سازی پیشرو کمیت‌سازهای وجودی φ_S با $\bar{n}$، ${f_S}^n$، $\overline{S^n}$ و $\bar{s}$ حقایق زیر را برای تأیید باقی می‌گذارد:

- $\mathcal{M} \models \bar{n} \in \omega$، بلافاصله توسط (i) از لم ۱.۴.
- کارکرد $f_S{}^n$، با ساخت $f_S{}^n$ ساده است.
- $\mathcal{M} \models f_S{}^n \gg \bar{n}$، بلافاصله توسط لم ۳.۴.
- $\mathcal{M} \models (\bar{n}\overline{S^n}) \in f_S{}^n$، دوباره با ساخت $f_S{}^n$.
- $\mathcal{M} \models (\bar{s}\bar{s}) \in \overline{S^n}$، با فرض $(s,s) \in S^n$.

□

لم ۵.۴. *اگر در یک مدل استاندارد $\mathcal{M}$ یک تقریب تابعی $f \gg k$ برای $k \in \omega$ وجود داشته باشد. با $f \in (kB)$، سپس برای همهٔ $p \in B$ وجود دارد $s,t : \mathbb{L}(\mathbb{B})$ با $p = (\bar{s},\bar{t})$ و $S \triangleright (s,t)$.*

اثبات. از آنجایی که $\mathcal{M}$ استاندارد است، $n : \mathbb{N}$ با $k = \bar{n}$ وجود دارد، بنابراین $f \gg \bar{n}$ و $(\bar{n}, B) \in f$ داریم. در هر مدل با $f \gg \bar{n}$ می‌توانیم نشان دهیم که $(\bar{k}\bar{S^k}) \in f$ با استقرا روی k، بنابراین به طور خاص $(\bar{n}, \bar{S^n}) \in f$ در $\mathcal{M}$. اما پس از آن با عملکرد f باید $B = \overline{S^n}$ باشد، بنابراین برای هر $p \in B$ ما در واقع $p \in \overline{S^n}$ داریم که استخراج $s,t : \mathbb{L}(\mathbb{B})$ با $p = (\bar{s},\bar{t})$ و $(s,t) \in S^n$ برای آن آسان است. سپس $S \triangleright (s,t)$ را با لم ۲.۴ نتیجه می‌گیریم. □

گزاره ۶.۴. *هر مدل استاندارد $\mathcal{M} \models Z'$ با $\mathcal{M} \models \varphi_S$، PCP S را تولید می‌کند.*

اثبات. یک مدل استاندارد از Z' با $\mathcal{M} \models \varphi_S$ یک تقریب تابعی $f \gg k$ برای $k \in \omega$ با یک مقدار $(k,B) \in f$ و $(x,x) \in B$. سپس توسط لم ۵.۴ وجود دارد $s,t : \mathbb{L}(\mathbb{B})$ با $(x,x) = (s,t)$ و $S \triangleright (s,t)$. با تزریق دوتایی‌های مرتب و رمزگذاری‌های رشته‌ای (iv)) از لم ۱.۴) t = s را به دست می‌آوریم و بنابراین $S \triangleright (s,s)$. □

گزاره ۷.۴. *اگر PCP S آنگاه $Z' \vdash \varphi_S$.*

قضیه ۸.۴. *فروکاهش‌های زیر را داریم:*

- *$PCP \preceq Z'$، مدلی استاندارد را که برای 'Z وجود دارد دربرمی‌گیرد.*
- *$PCP \preceq Z$، مدلی استاندارد را که برای Z وجود دارد دربرمی‌گیرد.*
- *$PCP \preceq ZF$، مدلی استاندارد را که برای ZF وجود دارد دربرمی‌گیرد.*

اثبات. با گزاره‌های ۴.۴، ۶.۴ و ۷.۴ و قضیهٔ ۶.۲ به دست می‌آید. □

دو گزارهٔ مرتبط در مورد نوع $\mathcal{M}$ درختان دارای پایه را می‌توان به صورت گسترش کلاس‌ها فرموله کرد؛ یعنی محمول‌های تکی، روی درختان (CE) و وجود یک عملگر توصیف برای کلاس های هم ریختی $[t]_{\approx}$ درختان (TD) :

$$CE := \forall(P, P' : \mathcal{T} \to \mathbb{P}).(\forall t.Pt \leftrightarrow P't) \to P = P'$$

$$TD := \exists(\delta : (\mathcal{T} \to P) \to \mathcal{P}).\forall P.(\exists t.P = [t]_{\approx}) \to P(\delta P)$$

نتیجه ۹.۴. *CE هم $PCP \preceq Z'$ و هم $PCP \preceq Z$ را نتیجه می‌دهد و $CE \wedge TD$ نتیجه می‌دهد $PCP \preceq ZF$.*

اثبات. CE و $CE \wedge TD$ مدل‌های مرتبه‌بالاتر Z و ZF را نمایش می‌دهند. به راحتی می توان نشان داد که آنها مدل های استاندارد هستند و گزاره‌سازی مرتبه اول Z و ZF را ارضا می‌کنند. □

قضیه ۱۰.۴. *با فرض LEM، کامل بودن هر پسوند $Z' \subseteq A$ که توسط یک استاندارد برآورده شده است این مدل به معنای تصمیم‌پذیری مسئلهٔ توقف ماشین‌های تورینگ است.*

اثبات. با نتیجهٔ ۹.۴، قضیهٔ ۶.۲ و گزارهٔ ۵.۲ به دست می‌آید. □

فصل ۵

نظریهٔ مجموعه‌های ZF بدون توابع اسکولِم

ما در نماد $\tilde{\Sigma} := (\_\_ \equiv \_\_, \_\_ \in \_\_)$ که فقط شامل تساوی و عضویت می‌شود کار می‌کنیم. برای بیان نظریهٔ مجموعه‌ها در این نحو، گزاره‌سازی‌های مشخص‌کننده نمادهای اسکولِم را دوباره فرموله می‌کنیم. در نماد قبلی Σ فقط برای اثبات وجود مجموعه‌های مربوطه استفاده می‌شود، به عنوان مثال:

$$\emptyset : \forall x.x \notin \emptyset \rightsquigarrow \exists u.\forall x.x \notin u$$

$$\mathcal{P}(x) : \forall xy.y \in \mathcal{P}(x) \leftrightarrow y \subseteq x \rightsquigarrow \forall x.\exists u.\forall y.y \in u \leftrightarrow y \subseteq x$$

به این ترتیب گزاره‌سازی‌های $\tilde{Z}'$، $\tilde{Z}$ و $\tilde{ZF}$ را به عنوان همتایان مربوط به Z ،Z' و ZF به دست می‌آوریم، . در این بخش، نشان می‌دهیم که این گزاره‌سازی‌های بدون نماد نیز همین کاهش از PCP را می‌پذیرند.

ایدهٔ غیررسمی تابع ترجمهٔ جایگزینی عبارت این است که $t : \mathcal{T}_\Sigma$ که با فرمول $\varphi_t : \mathbb{F}_{\tilde{\Sigma}}$ است. به عنوان مثال، شاخص $\times_0$ را به گونه‌ای توصیف می‌کند که مانند t رفتار کند:

$$\times_n \rightsquigarrow \times_0 \equiv \times_{n+1}$$
$$\emptyset \rightsquigarrow \forall \times_0 \notin \times_1$$
$$\mathcal{P}(t) \rightsquigarrow \exists \varphi_t[\times_0; \uparrow^2] \wedge \forall \times_0 \in \times_2 \leftrightarrow \times_0 \subseteq \times_1$$

فرمول $\mathcal{P}(t)$ ابتدا بیان می‌کند که مجموعه‌ای وجود دارد که φ_t را برآورده می‌کند (که در آن جانشینی $\uparrow^n$ همهٔ شاخص‌ها را با n تغییر می‌دهد) و سپس $\times_0$ را به عنوان مجموعهٔ توان آن مشخص می‌کند (با توجه به این دو کمیت به عنوان $\times_2$ ظاهر می‌شود). به طور مشابه، فرمول‌ها با نزول بازگشتی به اتم‌ها، که با فرمول‌هایی جایگزین می‌شوند که وجود مجموعه‌های مشخص‌شده را تأیید می‌کنند، ترجمه می‌شوند در رابطهٔ منظور، به عنوان مثال:

$$t \in t' \rightsquigarrow \exists \varphi_t[\times_0; \uparrow^2] \wedge \exists \varphi_{t'}[\times_0; \uparrow^3] \wedge \times_1 \in \times_0$$

اکنون تأیید می‌کنیم که ترجمهٔ $\tilde{\varphi}$ دو واقعیت مورد نظر را برآورده می‌کند، که از ساده‌تر شروع می‌شود. دلالت معنایی برای این منظور، مدل $\tilde{\Sigma}$ بدست آمده از یک مدل Σ را با $\tilde{\mathcal{M}}$ نشان می‌دهیم. $\mathcal{M}$ با فراموش کردن تفسیر نمادهای تابع موجود در $\tilde{\Sigma}$ عمل می‌کند. سپس برای یک مدل $\mathcal{M} \models Z'$، ارضاپذیری برای فرمول‌های ترجمه شده حفظ می‌شود، با توجه به اینکه این اصطلاح خصوصیات به طور منحصربه‌فردی از گزاره‌های 'Z ارضا می‌شوند، داریم:

لم ۱.۵. *فرض کنیم* $\mathcal{M} \models Z'$، $t : \mathbb{T}$، $\rho : \mathbb{N} \to \mathcal{M}$ و $x : \mathcal{M}$ *آنگاه داریم:* $x = \hat{\rho}t$ *اگر و تنها اگر* $(x; \rho) \models_{\tilde{\mathcal{M}}} \varphi_t$.

اثبات. با استقرا روی t با x تعمیم‌یافته به اثبات می‌پردازیم. ما فقط موارد $\times_n$ و $\emptyset$ را در نظر می‌گیریم:

- باید $x = \hat{\rho}\times_n$ اگر و تنها اگر $(x; \rho) \models_{\tilde{\mathcal{M}}} \times_0 \equiv \times_{n+1}$ را نشان دهیم که بنا به تعریف سریعاً به دست می‌آید.
- ابتدا با فرض $x = \emptyset$، باید نشان دهیم که $\forall y.y \notin x$، که بلافاصله از $\mathcal{M}$ است. اصل مجموعه تهی را برآورده می‌کند. برعکس با فرض $\forall y.y \notin x$ نتیجه می‌دهد $x = \emptyset$ که با استفاده از اصل توسعه‌پذیری $\mathcal{M}$ به دست می‌آید.

□

لم ۲.۵. *فرض کنیم* $\mathcal{M} \models Z'$، $\varphi : \mathbb{F}$ و $\rho : \mathbb{N} \to \mathcal{M}$ *آنگاه داریم:* $\rho \models_{\mathcal{M}} \varphi$ *اگر و تنها اگر* $\rho \models_{\tilde{\mathcal{M}}} \tilde{\varphi}$.

اثبات. با استقرا روی φ با ρ تعمیم‌یافته، همهٔ موارد به جز اتم‌ها مستقیماً استقرایی هستند. با در نظر گرفتن حالت $t \in t'$، ابتدا باید نشان دهیم که اگر $\hat{\rho}t \in \hat{\rho}t'$، آنگاه وجود دارد x و 'x با $x \in x'$ به ترتیب φ_t و $\varphi_{t'}$ ارضاکننده است. توسط لم ۱.۵ انتخاب $x := \hat{\rho}t$ و $x' := \hat{\rho}t'$ کافی است. حال برعکس، اگر چنین x و 'x وجود داشته باشد، توسط لم ۱.۵ ما می دانیم که $x = \hat{\rho}t$ و $x' = \hat{\rho}t'$ و به این ترتیب $\hat{\rho}t \in \hat{\rho}t'$ نتیجه می‌گیریم. مورد $t \equiv t'$ مشابه است. □

لم ۳.۵. *اگر* $\mathcal{M} \models Z'$ *آنگاه* $\tilde{\mathcal{M}} \models \tilde{Z}$.

اثبات. ما فقط باید گزاره‌های مربوط به عملیات مجموعه را در نظر بگیریم، جایی که ما کمیت‌کننده‌های وجودی معرفی‌شده در $\tilde{Z}'$ را با عملیات مربوطه موجود در $\mathcal{M}$ مثال بزنید . برای مثال، برای نشان دادن $\tilde{\mathcal{M}} \models \exists u.\forall x.x \notin u$ کافی است نشان دهیم که $\forall x.x \notin \emptyset$ در $\tilde{\mathcal{M}}$، که دقیقاً اصل مجموعه خالی است که توسط $\mathcal{M}$ ارضا شده است.

□

گزاره ۴.۵. *نتیجه می‌دهد* $\tilde{Z}' \models \tilde{\varphi}$ $Z' \models \varphi$.

اثبات. از لم ۲.۵ و ۳.۵ به دست می‌آید. □

لم ۵.۵. *برای هر* $t : \mathbb{T}$ *داریم* $\tilde{Z}' \vdash \exists\varphi_t$ *و* $\tilde{Z}' \vdash \varphi_t[x] \to \varphi_t[x'] \to x \equiv x'$.

اثبات. هر دو ادعا از طریق استقرا روی t هستند، دومی با x و x' تعمیم یافته است. دومی سریعاً برای متغیرها و $\emptyset$ به دست می‌آید، پس در مورد $\mathcal{P}(t)$ بحث می‌کنیم. با استقرا می‌دانیم $\tilde{Z}' \vdash \exists\varphi_t$ یک مجموعهٔ x را شبیه‌سازی می کند و باید $\tilde{Z}' \vdash \exists\exists\varphi_t[\times_0;\uparrow^2]\wedge\forall\times_0 \in \times_2 \leftrightarrow \times_0 \subseteq \times_1$ را نشان دهد. پس از نمونه‌سازی اولین کمیت با مجموعه u تضمین شده توسط قدرت وجودی گزاره‌ها را برای مجموعهٔ x و کمیت دوم با خود x تنظیم کنید، باید $\varphi_t[x]$ و $\forall\times_0 \in u \leftrightarrow \times_0 \in \times$ که هر دو با انتخاب x و u ساده هستند.
ادعای دوم از توسعه‌پذیری ناشی می‌شود که مشخصهٔ φ_t مجموعه‌های ارضاکننده دقیقاً با عناصر آنها را مشخص می‌کند. بنابراین در واقع گزاره‌های مربوط به عملیات مجموعه حتی در اثبات یکتایی استفاده نمی‌شود. □

لم ۶.۵. *برای هر* $\varphi : \mathbb{F}$ *و* $t : \mathbb{T}$ *داریم* $\tilde{Z}' \vdash \varphi_t[x] \to (\tilde{\varphi}[x] \leftrightarrow \widetilde{\varphi[x]})$.

اثبات. با استقرا روی φ، همهٔ موارد به جز اتم‌ها، با تکیه بر واقعیت، ساده هستند که ترجمه نحوی با تغییر نام متغیرها در موارد کمی کنش خوبی دارد. اثبات اتم‌ها به یک لم مشابه برای عبارت‌هایی که بیان می‌کند $\varphi_s[y;x]$ و $\varphi_{s[t]}[y]$ متکی است. هر زمان که $\varphi_t[x]$ قابل تعویض است، بقیه موارد ساده است. □

گزاره ۷.۵. *نتیجه می‌دهد* $\tilde{Z}' \vdash \tilde{\varphi}$ $Z' \vdash \varphi$.

اثبات. ما ادعای کلی تر را که $\Gamma + +Z' \vdash \varphi$ دلالت بر $\tilde{\Gamma} + +\tilde{Z}' \vdash \tilde{\varphi}$ را با استقرا اثبات می‌کنیم. در اشتقاق اول همهٔ قوانین به جز قانون فرض ،(A) ∀ـحذف (AE) و ∃ـحذف (EE) ساده است، ما دو مورد قبلی را توضیح می‌دهیم.

- اگر $\varphi \in \Gamma + +Z$، پس $\varphi \in \Gamma$ یا $\varphi \in Z'$. در حالت اول، $\tilde{\varphi} \in \tilde{\Gamma}$ داریم، بنابراین $\tilde{\Gamma} + +\tilde{Z}' \vdash \tilde{\varphi}$ توسط .(A) با توجه به مورد دوم، ما می توانیم $\tilde{Z}' \vdash \tilde{\varphi}$ را برای همه $\varphi \in Z'$ توسط اشتقاقات نسبتا خسته کننده با توجه به اندازه بزرگ برخی از ترجمه های بدیهیات. اگر $\Gamma + +Z' \vdash \varphi[t]$ از $\Gamma + +Z' \vdash \forall\varphi$ مشتق شده باشد، آنگاه با فرضیه استقرایی ما
- $\tilde{\Gamma} + +\tilde{Z}' \vdash \forall\tilde{\varphi}$ را بدانید. با توجه به لم ممکن است $\varphi_t[x]$ را برای یک متغیر x جدید فرض کنیم. سپس با مثال زدن فرضیه استقرایی به x از طریق (AE) $\tilde{\Gamma} + +\tilde{Z}' \vdash \tilde{\varphi}[x]$ و ادعای $\tilde{\Gamma} + +\tilde{Z}' \vdash \widetilde{\varphi[t]}$ را با لم ۶.۵ به پایان برسانید.

□

قضیه ۸.۵. *CE نتیجه می‌دهد $PCP \preceq \tilde{Z}'$ و $PCP \preceq \tilde{Z}$ و $CE \wedge TD$ نتیجه می‌دهد $PCP \preceq \widetilde{ZF}$.*

اثبات. مانند قضیهٔ ۶.۲ و گزاره‌های ۴.۵ و ۷.۵ اثبات می‌شود. □

قضیه ۹.۵. *منطق مرتبه اول با نماد دودویی رابطه تصمیم‌ناپذیر است.*

اثبات. با گزارهٔ ۷.۲ و فروکاهش $PCP \preceq \check{Z}'$ به دست می‌آید. □

فصل ۶

نتیجه‌گیری

در این رساله، ما یک رویکرد تألیفی برای فرمال و ماشینی کردنِ تصمیم‌ناپذیری و ناتمامیت منجر به منطق مرتبه اول را شرح داده‌ایم. رویکرد کلی این بود که در دو مطالعه موردی، یکی با نظریه‌های حسابی در خانوادهٔ PA مورد بررسی قرار گرفت؛ چرا که PA یکی از نظام‌های معمول برای درک ناتمامیت در نظر گرفته می‌شود و بررسی دیگر در مورد نظریهٔ مجموعه‌های ZF به عنوان یکی از پایه‌های استاندارد ریاضیات بود. راهبرد انتخاب شده مکمل شواهد ماشینی‌کردن بسیار دشوارتر بر اساس جملات گودل و برای ZF انتخاب PCP به عنوان مسئلهٔ اصلی به جای (H_{10}) یا PA، ساده‌سازی موضوع است؛ چراکه تنها به یک بازگشت نیاز دارد.

همانطور که به طور فرمال در تعریف ۸ بیان شد، ما ناتمامیت را به عنوان یک ویژگی نظام استنتاجی کلاسیک در نظر می‌گیریم. اگرچه به طور کلی که به احتمال زیاد ضعیف‌تر است، ناتمامیت نظام استنتاج شهودگرایی نیز می‌تواند یک ویژگی معنی‌دار در نظر گرفته شود و به ظریق مشابهی دنبال شود. به طور مشخص، نسخهٔ مربوط به گزارهٔ ۹ که برای مفهوم شهودی صادق است، انواع قضایای ۲۶ و ۳۶ بدون LEM قابل اثبات هستند.

هم‌چنین دلالت معنایی $\mathcal{T} \models \varphi$ را تعریف می‌کنیم؛ بدون اینکه مدلمان را به مدل‌های کلاسیک محدود کنیم، یعنی مدل‌هایی که تمام نمونه‌های مرتبه اول را برآورده می‌کنند. در فراتئوری ساختنی ما، این کار لازم است تا بتوانیم از مدل‌های استاندارد PA و ZA، که فقط در یک فراتئوری کلاسیک هستند استفاده کنیم.

به طور مشابه، ما مشخص نمی کنیم که آیا PA و ZF به عنوان نظریه‌های کلاسیک دیده می‌شوند یا به عنوان همتایان شهودی آن‌ها، یعنی حساب هیتینگ و گونه‌ای از نظریهٔ مجموعه‌های شهودی. با انتخاب عدم تمایز صریح بین این‌ها توسط LEM به عنوان طرح گزارهٔ مرتبه اول، تشخیص این تمایز را به نظام استنتاج می‌سپاریم تا بین هر دو دیدگاه تمایز قائل شود. برای سادگی نیز، ما تصمیم گرفتیم فقط از PA و ZF در متن اصلی صحبت کنیم؛ به ویژه از آنجایی که بحث در مورد نظریهٔ مجموعه‌های شهودی شامل انتخاب یک نظام خاص است.

کتاب‌نامه

[**1**] Dominik, Kirst and Hermes, Marc. “Synthetic Undecidability and Incompleteness of First-Order Axiom Systems in Coq.” ITP (2021).
[**2**] Sterling, Jonathan. (2021). First Steps in Synthetic Tait Computability: The Objective Metatheory of Cubical Type Theory [Zenodo].
[**3**] Forster, Yannick. (2022). Parametric Church’s Thesis: Synthetic Computability Without Choice. In: Artemov, S., Nerode, A. (eds) Logical Foundations of Computer Science. LFCS 2022. Lecture Notes in Computer Science(), vol 13137. Springer, Cham.

Abstract

We mechanise the undecidability of various first-order axiom systems in Coq, employing the synthetic approach to computability underlying the growing Coq Library of Undecidability Proofs. Concretely, we cover both semantic and deductive entailment in fragments of Peano arithmetic (PA) and Zermelo-Fraenkel set theory (ZF), with their undecidability established by many-one reductions from solvability of Diophantine equations, i.e. Hilbert's tenth problem (H10), and the Post correspondence problem (PCP), respectively. In the synthetic setting based on the computability of all functions definable in a constructive foundation, such as Coq's type theory, it suffices to define these reductions as meta-level functions with no need for further encoding in a formalised model of computation. The concrete cases of PA and ZF are prepared by a general synthetic theory of undecidable axiomatisations, focusing on well-known connections to consistency and incompleteness. Specifically, our reductions rely on the existence of standard models, necessitating additional assumptions in the case of full ZF, and all axiomatic extensions still justified by such standard models are shown incomplete. As a by-product of the undecidability of ZF formulated using only membership and no equality symbol, we obtain the undecidability of first-order logic with a single binary relation.

College of Science
School of Mathematics, Statistics, and Computer Science

Synthetic Undecidability and Incompleteness of First-Order Axiom Systems in Coq

Sajede Talebi

Supervisor: Dr. Mojtaba Mojtahedi

A thesis submitted to Graduate Studies Office
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

2022