دانشگاه تبریز

دانشکده علوم ریاضی

گروه ریاضی محض

پایان‌نامه

برای دریافت درجه کارشناسی ارشد در رشته‌ی

ریاضی محض، گرایش منطق

عنوان

برهان‌های قضایای ناتمامیت بر اساس پارادوکس بِری

استاد راهنما

دکتر سعید صالحی پور مهر

استاد مشاور

هژیر حومئی

پژوهشگر

سونیا سروری مهرآباد

۱۳۹۴

بسم الله الرّحمن الرّحیم

سپاس خدایی را که سخنوران در ستودن او بمانند و شمارگران شمردن نعمتهای او ندانند، و کوشندگان، حقّ او را گزاردن نتوانند. خدایی که پای اندیشهٔ تیزگام در راه شناسایی او لنگ است، و سر فکرت ژرف رو به دریای معرفتش بر سنگ. صفتهای او تعریف ناشدنی است و به وصف درنیامدنی، و در وقت ناگنجیدنی، و به زمانی مخصوص نابودنی. به قدرتش خلایق را بیافرید، و به رحمتش بادها را بپراکنید، و با خرسنگها لرزهٔ زمین را در مهار کشید.

گواهی می‌دهم که خدا یکتاست، انبازی ندارد و بی‌همتاست. گواهیی از روی اعتقاد و ایمان، بی‌آمیغ برآمده از امتحان؛ و گواهی می‌دهم که محمّد (ص) بندهٔ او و پیامبر اوست. او را بفرستاد با دینی آشکار، و با نشانه‌هایی پدیدار، و قرآنی نبشته در علم پروردگار. که نوری است رخشان، و چراغی است فروزان، و دستورهایش روشن و عیان. تا گرد دودلی از دلها بزداید، و با حجّت و دلیل ملزم فرماید.

پاک خدایا! چه بزرگ است آنچه می‌بینیم از خلقت تو؛ و چه خرد است، بزرگی آن در کنار قدرت تو؛ و چه با عظمت است آنچه می‌بینیم از ملکوت تو، و چه ناچیز است برابر آنچه بر ما نهان است از سلطنت تو، و چه فراگیر است نعمت تو در این جهان؛ و چه اندک است در کنار نعمتهای آن جهان.

خدایا! اگر در پرسش خود درمانم یا راه پرسیدن را ندانم، صلاح کارم را به من نما و دلم را بدانچه رستگاری من در آن است متوجه فرما! که چنین کار از راهنماییهای تو ناشناخته نیست و از کفایتهای تو نه.

از فرمایشات حضرت علی (ع)

تقدیم به:

پدر و مادر عزیزتر از جانم

و همسرم که عاشقانه دوستش دارم

بنام خدا

ومن لم یشکر المخلوق لم یشکر الخالق.

حمد و سپاس ارزانی بارگاه حضرت احدیت که آثار قدرت او بر چهره روز روشن، تابان است و انوار حکمت او در دل شب تار، درفشان. آفریدگاری که خویشتن را به ما شناساند و درهای علم را بر ما گشود و عمری و فرصتی عطا فرمود تا بدان، بنده ضعیف خویش را در طریق علم و معرفت بیازماید. در آغاز وظیفه‌ی خود می‌دانم از زحمات بی دریغ استاد راهنمای خود، جناب آقای دکتر **سعیــــد صالحـــی پـــورمهـــر**، صمیمانه تشکر و قدردانی نمایم که قطعاً بدون راهنمایی‌های ارزنده‌ی ایشان این مجموعه به انجام نمی‌رسید.

از جناب آقای **دکترهژیر حومئی** که زحمات مطالعه و مشاوره‌ی این رساله را تقبل فرمودند و در آماده سازی این رساله به نحو احسن اینجانب را مورد راهنمایی قرار دادند، کمال امتنان را دارم.

از جناب آقای دکتر **جعفـــر صـــادق عیـــوضلـــو** که داوری این رساله را با نهایت دقت و صرف وقت زیاد انجام دادند، تشکر می‌نمایم.

از جناب آقای دکتر **کریمی** و جناب آقای **سراجی** که در تدوین این رساله کمک شایانی به اینجانب نمودند و همچنین از تمام دوستان دوران تحصیلم کمال قدردانی و تشکر را دارم. ازکلیه دبیران دوران تحصیلم، اساتید گرامی بخصوص دکتر **اصغـــر رنجبـــری** مدیرگروه ریاضی محض و نیز کارکنان محترم دانشکده‌ی علوم ریاضی و تحصیلات تکمیلی دانشگاه تبریز که در مدت تحصیلات دانشگاهی اینجانب زحمات فراوانی را متحمل شده‌اند، تشکر می‌نمایم.

بوسه بر دستان پدر ومادر عزیزم می‌زنم که صبورانه رنج سال‌های تحصیل مرا تحمل کردند واندرزـ های‌شان همیشه روشنگر راهم بوده و خواهد بود انشاالله.

و سپاس و سپاس از همسر مهربانم که وجودش التیام‌بخش لحظه‌های سختی بود که سپری شد و عاشقانه مرا در این راه یاری کرد.

در پایان از کلیه اعضای خانواده‌ام، خواهرانم و برادر عزیزم که در تمامی مراحل همواره یار و مشوق من بوده‌اند، سپاسگزاری می‌کنم.

سونیا سروری مهرآباد

۱۳۹۴

نام خانوادگی دانشجو: سروری مهرآباد نام: سونیا
عنوان: برهان‌های قضایای ناتمامیت بر اساس پارادوکس بِری
استاد راهنما : دکتر سعید صالحی پور مهر استاد مشاور : هژیر حومئی
مقطع تحصیلی: کارشناسی ارشد رشته: ریاضی محض گرایش: منطق دانشگاه تبریز دانشکده علوم ریاضی تاریخ فارغ التحصیلی: ۱۳۹۴ تعداد صفحات: ۴۶
کلید واژه‌ها: قضیه ناتمامیت، پارادوکس بری، پیچیدگی کولوموگروف.

چکیده

طی سال های ۱۹۶۰ تا ۱۹۸۰ شایتین[۱]، بولوس[۲] و وپنکا[۳] با استفاده از صوری‌سازی پارادوکس بری، اثبات‌های جدیدی برای قضایای ناتمامیت ارایه نمودند. در این پایان‌نامه، به مطالعه دقیق این اثبات‌ها پرداخته و روابط بین آنها را بررسی می‌نماییم. نشان داده می‌شود که می‌توان از لم قطری نیز برای اثبات قضیه ناتمامیت بر اساس پارادوکس بری استفاده نمود. همچنین با تعریف یک پیچیدگی کولموگروف مناسب، می‌توان نشان داد که برهان بولوس به نوعی، گونه‌ای از برهان شایتین است.

۱ Chaitin

۲ Boolos

۳ Vopěnka

فهرست مطالب

مقدمه

گودل[۴] در مقاله مشهور [۶] بیان می‌دارد که شباهت‌هایی بین پارادوکس دروغگو و جمله مستقل ارایه شده در برهان وی وجود دارد. برهان‌های قضیه ناتمامیت مبتنی برصوری‌سازی پارادوکس بِری[۵] توسط شایتین [۵] و بولوس [۳] ارایه شده‌اند. پارادوکس بِری بر مبنای جمله «کمترین عدد صحیح که در کمتر از ۹۰ نماد نمی‌توان آنرا توصیف کرد» بنا نهاده شده است؛ اما عبارت درون نقل‌قول، خود یک توصیف ۸۰ نمادی است! این پارادوکس در قرن بیستم توسط راسل [۱۹] معرفی شد. در سال ۱۹۷۰ شایتین قضیه اول ناتمامیت را به وسیله صوری‌سازی پارادوکس بِری با استفاده از پیچیدگی کولموگروف [۶] ثابت کرد. بولوس شکل ضعیفی از قضیه ناتمامیت اول را در سال ۱۹۸۰ با صوری‌سازی پارادوکس بِری در نظریه حساب ثابت کرد. برهان بولوس توسط کیکوکچی و تاناکا [۱۲] و کیکوچی [۱۰] تعمیم داده شد. به طور خاص، کیکوچی قضیه دوم ناتمامیت را با به کار بردن فن نظریه مدلی کرایسل به دست آورد. وی هم‌چنین در [۱۱] قضیه دوم ناتمامیت را با بررسی پیچیدگی کولوموگروف ثابت کرد. روابط بین این برهان‌ها موضوع مورد بحث این پایان‌نامه است. یکی از ویژگی‌های رایج برهان‌های مبتنی بر پارادکس بِری برای قضایای ناتمامیت که بولوس تاکید کرده، این است که آنها از لم قطری صریحا استفاده نمی‌کنند. در مقابل، تفاوت بین چنین برهان‌هایی با برداشت‌های متفاوت آنها از مفهوم «توصیف» مشخص می‌شود: شایتین و کیکوچی از پیچیدگی کولموگروف، بولوس از مدل استاندارد نظریه حساب وکیکوچی از اثبات‌پذیری در حساب

[۴] Gödel

[۵] Berry

[۶] Kolomogorow

استفاده کرده‌اند. در این پایان‌نامه، که بر اساس مقالات [۱۳] و [۷] تنظیم شده است، ما به دقت برهان‌های بالا را بررسی کرده و روابط بین آنها را نمایان خواهیم کرد. بدین منظور جمله مستقل در برهان کیکوچی را با استفاده از لم قطری به دست آورده و نشان داده خواهد شد که قضیه دوم ناتمامیت از صوری‌سازی کیکوچی از پارادوکس بِری می‌تواند بدون استفاده از فنون نظریه مدلی ثابت شود. این نتیجه می‌دهد که تفاوتی بین استفاده کردن یا نکردن از لم قطری برای برهان‌های مبتنی بر پارادوکس بِری وجود ندارد. سپس نشان داده می‌شود که برهان کیکوچی به نوعی، گونه‌ای از برهان شایتین است، جایی که مفهومی مناسب از پیچیدگی کولموگروف با استفاده از اثبات‌پذیری در حساب تعریف شده است. و در آخر، توصیفی از وجود یک ماشین تورینگ جهانی ارایه می‌دهیم به طوری که $c_{\mathbf{T}} \neq c_{\mathbf{S}}$ $\left(c_T = min\{x \mid \forall w : T \nvdash K(w) > x\}\right)$ برقرار باشد: ثابت خواهد شد که $c_{\mathbf{S}} < c_{\mathbf{T}}$ برای برخی از ماشین‌های تورینگ جهانی برقرار است اگر و فقط اگر $\mathbf{T}$ یک Π_1ـ جمله حسابی را ثابت کند که $\mathbf{S}$ نمی‌تواند آن را ثابت کند. ثابت دیگر $r_{\mathbf{T}}$ توسط راتیکاینن[۷] در ارتباط با $c_{\mathbf{T}}$ معرفی شده است. ما نشان می‌دهیم که تفاوت بین $c_{\mathbf{T}}$ و $r_{\mathbf{T}}$ می‌تواند به هر اندازه دلخواه بزرگ باشد. از طرف دیگر، برای برخی ماشین‌های تورینگ جهانی $r_{\mathbf{S}} < r_{\mathbf{T}}$ برقرار است اگر و فقط اگر برای برخی ماشین‌های تورینگ جهانی (احتمالاً متفاوت) $c_{\mathbf{S}} < c_{\mathbf{T}}$ برقرار باشد.

[۷] Raatikainen

فصل ۱

پیشینه پژوهش و مفاهیم مقدماتی

در سراسر این پایان‌نامه زبان حساب را با نماد L_A مشخص می‌کنیم. در این زبان مرتبه اول $L_A = \{+, \times, S, 0, <\}$، $+$ و $\times$ نمادهای تابعی دو موضعی، S یک نماد تابعی یک موضعی، 0 نماد ثابت و $<$ یک نماد رابطه‌ای دو موضعی می‌باشد. از نمادهای $v_۰, v_۱, \ldots$ به عنوان متغیر در L_A استفاده می‌کنیم بدین گونه که، برای $j < i$ اگر یک متغیر v_j وجود داشته باشد که در فرمول استفاده نشده است نباید متغیر v_i در فرمول ظاهر شود. منظور از یک مدل استاندارد برای حساب عبارت است از یک L_A ساختار با جهان $\mathbb{N} = \{0,1,2,\ldots\}$ که در آن نمادهای L_A دارای تعابیر استاندارد می‌باشند. برای هر $n \in \mathbb{N}$، منظور از $\overline{n}$ عبارت است از ترم $S(S(\ldots S(0)\ldots))$ که در واقع از اثر دادن تابع تالی به تعداد n بار روی نماد 0 بدست می‌آید. منظور از طول یک فرمول در حساب، تعداد نمادهایی است که در آن فرمول استفاده شده‌اند. طول فرمول φ را با نماد $|\varphi|$ و عدد گودل φ را با $\ulcorner\varphi\urcorner$ نشان می‌دهیم. حساب پئانو [۱] $\mathtt{PA}$ را با نمایش می‌دهیم و $\mathbf{T}$ را توسیعی به طور بازگشتی اصل‌پذیر از $\mathtt{PA}$ در نظر می‌گیریم.

تعریف ۱.۰.۱. یک فرمول φ در L_A، Δ_0 نامیده می‌شود هرگاه همه سورهای آن کراندار (به صورت $\forall x \leq t$ یا $\exists x \leq t$) باشند، و Σ_1 نامیده می‌شود هرگاه به شکل $(\exists x_۱, \ldots, \exists x_k)\psi$ برای Δ_0 فرمول ψ باشد.

لم ۲.۰.۱. *هرگاه φ یک Σ_1 فرمول باشد، آنگاه $(\exists x < t)\varphi$ و نیز $(\forall x < t)\varphi$ معادل یک Σ_1 فرمول می‌باشند.*

برهان. فرض کنید $\varphi = (\exists z)\psi(x, t, z)$ که ψ، یک $\Delta_۰$ فرمول می‌باشد. نشان می‌دهیم که

$$(\forall x \leqslant t)\varphi \equiv (\forall x \leqslant t)(\exists z)\psi(x, t, z) \equiv (\exists w)(\forall x \leqslant t)(\exists z \leqslant w)\psi(x, t, z) \in \Sigma_۱$$

استنتاج چپ به راست بدیهی است. برای طرف دیگر فرض کنید $(\exists z)\psi(k, t, z)$ برای هر $k \leqslant t$ برقرار است. پس qای پیدا می‌کنیم که

$$\mathbb{N} \vDash (\forall x \leqslant t)(\exists z \leqslant \overline{q})\psi(x, t, z).$$

[۱] Peano

در حالت کلی با استقرا روی i که $i = 0, 1, \ldots, t$ نشان می‌دهیم q_iای وجود دارد به طوری که

$$\mathbb{N} \vDash (\forall x \leqslant \bar{i})(\exists z \leqslant \bar{q}_i)\psi(x, i, z).$$

برای ۰ $= i$ حکم بدیهی است. فرض کنید حکم برای i برقرار باشد، حال نشان می‌دهیم حکم برای ۱ $+ i$ نیز برقرار است. r را چنان در نظر بگیرید که $\mathbb{N} \vDash \varphi(\overline{i+۱}, t, r)$. در اینصورت قرار دهید $q_{i+۱} = max(q_i, r)$. به وضوح حکم برای ۱ $+ i$ نیز برقرار می‌شود. □

فرض کنید $\mathsf{Pr}_{\mathbf{T}}(x)$ یک Σ_1 فرمول استاندارد باشد که اثبات‌پذیری در $\mathbf{T}$ را بیان می‌کند. جمله $\mathsf{Con}(\mathbf{T})$ سازگاری $\mathbf{T}$ را ادعا می‌کند و معادل $\neg\mathsf{Pr}_{\mathbf{T}}(\ulcorner \overline{0} = \overline{1} \urcorner)$ تعریف می‌شود. نظریه $\mathbf{T}$ را Σ_1 درست نامند اگر Σ_1 فرمول φ غلط وجود نداشته باشد به طوری که $\mathbf{T} \vdash \varphi$.
برای اثبات قضایا و لم زیر می‌توانید به مرجع [۴] مراجعه کنید.

لم ۳.۰.۱. *(لم قطری سازی) برای هر فرمول $\varphi(x, y)$ که همه متغیرهای آزاد آن ازبین x و y هستند، فرمول $\psi(v_۰)$ با تنها متغیر آزاد $v_۰$ وجود دارد به طوری که*

$$\mathbf{T} \vdash \forall x \big(\psi(x) \longleftrightarrow \varphi(x, \ulcorner \psi(v_۰) \urcorner)\big).$$

قضیه ۴.۰.۱. *(شرایط اثبات‌پذیری هیلبرت برنِی لُب[۲]) برای هر جمله φ و ψ داریم:*

(۱) $\mathbf{T} \vdash \varphi \Longrightarrow \mathbf{T} \vdash \mathsf{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner);$

(۲) $\mathbf{T} \vdash \mathsf{Pr}_{\mathbf{T}}(\ulcorner \varphi \longrightarrow \psi \urcorner) \longrightarrow \big(\mathsf{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \longrightarrow \mathsf{Pr}_{\mathbf{T}}(\ulcorner \psi \urcorner)\big);$

(۳) $\mathbf{T} \vdash \mathsf{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \longrightarrow \mathsf{Pr}_{\mathbf{T}}(\ulcorner \mathsf{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \urcorner).$

قضیه ۵.۰.۱. *برای هر Σ_1 جمله φ داریم:*

(۱) *اگر φ درست باشد آنگاه $\mathbf{T} \vdash \varphi$؛*

(۲) $\mathbf{T} \vdash \varphi \longrightarrow \mathsf{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner)$.

[۲] Hilbert-Bernays-Löb

توجه کنید که قسمت (۱) در قضیه بالا را Σ_1 تمامیت و قسمت (۲) را Σ_1 تمامیت صوری شده می‌نامیم.

فرض کنید f و g توابع بازگشتی و m یک عدد طبیعی باشد. می‌نویسیم $f(m)\downarrow$ اگر $f(m)$ تعریف شده باشد در غیر اینصورت می‌نویسیم $f(m)\uparrow$. هم چنین می‌نویسیم $f(x) \simeq g(x)$ اگر برای هر $n \in \mathbb{N}$، هر دو $f(n)$ و $g(n)$ تعریف نشده باشند یا اگر تعریف شده باشند آنگاه $f(n) = g(n)$. یک رابطه در $\mathbb{N}$ را بازگشتی گوییم اگر تابع مشخصه آن بازگشتی باشد. برای یک رابطه $R(x,y)$ روی $\mathbb{N}$، $\mu_y[R(x,y)]$ یک تابع جزئی است به طوری که برای هر $m \in \mathbb{N}$،

$$\mu_y[R(m,y)]\downarrow \quad \Longleftrightarrow \quad \text{برای هر } k \leq n \text{ } R(m,k) \text{ تعریف شده باشد}$$

به طوری که

$$\mu_y[R(m,y)] = \text{کوچکترین } k \text{ که } R(m,k) \text{ برقرار باشد}$$

توجه کنید که اگر $R(x,y)$ یک رابطه بازگشتی در $\mathbb{N}$ باشد $\mu_y[R(x,y)]$ یک تابع بازگشتی است. تابع بازگشتی تام یک موضعی $(x)_n$ برابر نمای n ــ امین عدد اول در تجزیه عامل‌های اول x تعریف شده است. تابع $\langle \cdot , \cdot \rangle : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$ یک دوسویی بازگشتی متعارف است و تابع $[x]_i : \mathbb{N} \longrightarrow \mathbb{N}$ توابع تصویری بازگشتی هستند به طوری که

$$\forall a_0, a_1 \in \mathbb{N}; \quad [\langle a_0, a_1\rangle]_0 = a_0, \quad [\langle a_0, a_1\rangle]_1 = a_1.$$

فرض کنید f یک تابع با دامنه $\mathbb{N}$ باشد. اگر فرمول $\varphi(x,y)$ وجود داشته باشد به طوری که برای هر $m,n \in \mathbb{N}$،

$$f(m) = n \Longleftrightarrow \mathbf{T} \vdash \varphi(\overline{m},\overline{n}) \wedge \forall v_0 \forall v_1 \big(\varphi(\overline{m},v_0) \wedge \varphi(\overline{m},v_1) \longrightarrow v_0 = v_1\big)$$

در اینصورت گوییم f در $\mathbf{T}$ نمایش‌پذیر است.

گزاره ۶.۰.۱. *فرض کنید f یک تابع با دامنه $\mathbb{N}$ باشد. آنگاه f یک تابع بازگشتی است اگر وتنها اگر f در $\mathbf{T}$ نمایش‌پذیر باشد.*

اثبات گزاره بالا را به عنوان مثال در [۸] و [۴] می‌توان یافت. پارادوکس بری می‌تواند در مجموعه فرمول‌ها بوسیله بیان کردن مفهوم «توصیف» صوری شود. شرح ذیل فرمول‌بندی بولوس از مفهوم توصیف در [۳] است.

تعریف ۷.۰.۱. فرض کنید $n \in \mathbb{N}$ و $\varphi(v_0)$ یک فرمول با تنها متغییر آزاد v_0 باشد. گوییم $\varphi(v_0)$ توصیف n است اگر

$$\mathbb{N} \vDash \varphi(\overline{n}) \wedge \forall v_0 \forall v_1 \big(\varphi(v_0) \wedge \varphi(v_1) \longrightarrow v_0 = v_1\big).$$

در این فرمول‌بندی هر عدد طبیعی می‌تواند توسط چندین فرمول توصیف شود اما هر فرمول حداکثر یک عدد طبیعی را توصیف می‌کند. بولوس بوسیله این فرمول‌بندی، قضیه ناتمامیت را با استفاده از صوری سازی پارادوکس بری اثبات کرد.

قضیه ۸.۰.۱. *هیچ الگوریتمی وجود ندارد که همه جملات درست حساب را محاسبه کند.*

باروایس[۳] در مقاله [۲] از برهان بولوس این چنین تعریف می‌کند: «بسیار دوست داشتنی و آسان‌ترین برهان از قضیه ناتمامیت دوم که من همواره دیدم». در حالی که ماهیرا[۴] در مقاله [۱۷] پافشاری کرد که قضیه بولوس متفاوت از قضیه گودل در سه چیز است:

(۱) قضیه بولوس مفهوم درستی را مدنظر قرار می‌دهد در حالی که قضیه گودل این چنین نیست؛

(۲) قضیه بولوس ضعیف تر از قضیه ناتمامیت اصلی گودل است؛

(۳) در نتیجه نمی‌توان قضیه ناتمامیت دوم را از قضیه بولوس به روش استاندارد به دست آورد.

[۳] Barwise

[۴] maehara

فصل ۲

برهان‌های قطری شده

کیکوچی[۱] ([۱۰]) فرمول‌بندی بولوس از مفهوم «توصیف» را با قرار دادن «اثبات‌پذیری» به جای «درستی» در تعریف، تغییر داد.

تعریف ۹.۰.۲. (کیکوچی [۱۰]) فرض کنید $n \in \mathbb{N}$ و $\varphi(v_\circ)$ یک فرمول با تنها متغییر آزاد $v_\circ$ باشد. گوییم $\varphi(v_\circ)$ توصیف n در نظریه $\mathbf{T}$ است اگر

$$\mathbf{T} \vdash \varphi(\overline{n}) \wedge \forall v_\circ \forall v_\backslash \big(\varphi(v_\circ) \wedge \varphi(v_\backslash) \longrightarrow v_\circ = v_\backslash\big).$$

با استفاده از این تعریف، کیکوچی قضیه ناتمامیت را در شکل اصلی آن بوسیله فرمول‌بندی پارادوکس بری و بدون استفاده از لم قطری اثبات کرد، و صورت نظریه مدلی قضیه ناتمامیت دوّم را نتیجه گرفت. در این قسمت، نشان می‌دهیم که جمله مستقل در برهان مقاله کیکوچی [۱۰] را می‌توان با استفاده از لم قطری به دست آورده و قضیه ناتمامیت دوم را بدون استفاده از نظریه مدل ثابت کرد. لم زیر صورتی از لم قطری است که از آن در برهان قضیه ناتمامیت استفاده می‌کنیم.

لم ۱۰.۰.۲. *(لم قطری‌سازی نسبت به طول) برای هر فرمول $\varphi(x,y)$ که تنها متغیرهای آزاد آن x یا y هستند، فرمول $\psi(v_\circ)$ با تنها متغیر آزاد $v_\circ$ وجود دارد به طوری که*

$$\mathbf{T} \vdash \forall x \Big(\psi(x) \longleftrightarrow \varphi(x, |\psi(v_\circ)|)\Big).$$

برهان. فرض کنید $lh(x,y)$ یک نمایش دهنده تابع بازگشتی

«y = طول یک فرمول که عدد گودل آن x است»

باشد. با استفاده از لم قطری سازی، یک فرمول $\psi(v_\circ)$ با تنها متغییر آزاد $v_\circ$ وجود دارد به طوری که $\mathbf{T} \vdash \forall x \Big(\psi(x) \longleftrightarrow \exists z \Big[\varphi(x,z) \wedge lh(\ulcorner \psi(v_\circ) \urcorner, z)\Big]\Big)$. حال

$$\mathbf{T} \vdash \forall x \Big(\varphi(x, |\psi(v_\circ)|) \longleftrightarrow \exists z \big(\varphi(x,z) \wedge lh(\ulcorner \psi(v_\circ) \urcorner, z)\big)\Big)$$

[۱] Kikuchi

برقرار است زیرا قسمت $\mathbf{T} \vdash \forall x\Big(\varphi(x, |\psi(v_\circ)|) \longrightarrow \exists z\big(\varphi(x,z) \wedge lh(\ulcorner\psi(v_\circ)\urcorner, z)\big)\Big)$ بدیهی بوده و از طرفی بنابه تعریف $lh(x,y)$ چون z طول یک فرمولی است که $\ulcorner\psi(v_\circ)\urcorner$ عدد گودل آن است پس قسمت عکس آن یعنی

$$\mathbf{T} \vdash \exists z\big(\varphi(x,z) \wedge lh(\ulcorner\psi(v_\circ)\urcorner, z)\big) \longrightarrow \varphi(x, |\psi(v_\circ)|)$$

نیز برقرار است. لذا نتیجه می‌گیریم که $\mathbf{T} \vdash \forall x\Big(\psi(x) \longleftrightarrow \varphi(x, |\psi(v_\circ)|)\Big)$. $\square$

توجه کنید که این لم را می‌توان به طور مستقیم و بدون استفاده از لم قطری به دست آورد:

برهان. فرض کنید l طول فرمول $\alpha(x,y) \equiv \forall z\big(z = \overline{4} \cdot y \longrightarrow \varphi(x,z)\big)$ باشد، و $\psi(v_\circ)$ را برابر $\alpha(v_\circ, \overline{l})$ قرار دهید. طول $\overline{n}$ برابر $3n+1$ است به دلیل این که

$$.\overline{n} = \underbrace{SSS\cdots S}_{n\text{بار}}(0)$$

از آنجا که نماد y دقیقاً در یک مکان در فرمول $\alpha(x,y)$ رخ می‌دهد، طول فرمول $\psi(v_\circ)$، برابر عدد $l - 1 + (3l+1) = 4l$ است. بنابراین $\mathbf{T} \vdash \forall x\big(\psi(x) \longleftrightarrow \varphi(x, |\psi(v_\circ)|)\big)$. $\square$

حال قضیه اول ناتمامیت گودل را اثبات می‌کنیم. فرض کنید $\nu(\ulcorner\varphi(v_\circ)\urcorner, n)$ عدد گودل جمله $\varphi(\overline{n}) \wedge \forall v_\circ \forall v_1 \big(\varphi(v_\circ) \wedge \varphi(v_1) \longrightarrow v_\circ = v_1\big)$، و $\mathsf{Fml\text{-}Lh}(x,y)$ یک Σ_1 فرمول نمایش دهنده رابطه بازگشتی زیرباشد:

«x عددگودل یک فرمولی است که طول آن کمتر یا مساوی y است».

فرض کنید $\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(x,y)$ فرمول

$$\exists z\big(\mathsf{Pr}_{\mathbf{T}}(\nu(z,x)) \wedge \mathsf{Fml\text{-}Lh}(z,y)\big)$$

و μ-unDef$_{\mathbf{T}}$-Lh(x,y) فرمول

$$\neg\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(x,y)\wedge\forall z<x\,\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,y)$$

باشد. توجه داشته باشید که فرمول Def$_{\mathbf{T}}$-Lh(x,y) معادل یک Σ_1 فرمول است زیرا هر دو $\mathsf{Pr}_T\big(\nu(z,x)\big)$ و Fml-Lh(z,y)، Σ_1 فرمول هستند. بنابراین فرمول $\forall z<x\,$Def$_{\mathbf{T}}$-Lh(z,y) نیز Σ_1 فرمول است. فرمول Def$_{\mathbf{T}}$-Lh(x,y) می‌گوید که «فرمولی با طول y یا کمتر وجود دارد به طوری که عدد x را توصیف می‌کند» و μ-unDef$_{\mathbf{T}}$-Lh(x,y) بیان می‌کند که «xکوچکترین عدد طبیعی است که نمی‌تواند توسط هیچ فرمولی با طول y یا کمتر توصیف شود». طبق لم ۱۰.۰.۲، فرمول $\sigma(v_\circ)$ با تنها متغییر آزاد $v_\circ$ وجود دارد به طوری که $\mathbf{T}\vdash\forall x\big(\sigma(x)\longleftrightarrow\mu\text{-unDef}_{\mathbf{T}}\text{-Lh}(x,|\sigma(v_\circ)|)\big)$. فرض کنید $e\in\mathbb{N}$ طول فرمول $\sigma(v_\circ)$ باشد. توجه کنید که چون L_A شامل حداکثر تعداد متناهی نماد نامنطقی می‌باشد، پس تعداد متناهی عدد توصیف شده توسط فرمول با طول e یا کمتر وجود دارد. بنابراین فرض می‌کنیم m_e کوچک‌ترین عدد طبیعی باشد که نمی‌تواند توسط فرمولی با طول e یا کمتر توصیف شود. بنابراین جمله $\forall z<\overline{m_e}\,Def_{\mathbf{T}}$-Lh$(z,\overline{e})$ درست بوده و چون معادل با یک Σ_1جمله درست است، لذا در T اثبات‌پذیر است.

قضیه ۱۱.۰.۲. *(۱) اگر $\mathbf{T}$ سازگار باشد، آنگاه* $\mathbf{T}\nvdash\sigma(\overline{m_e})$؛
(۲) اگر $\mathbf{T}$، Σ_1 درست باشد، آنگاه $\mathbf{T}\nvdash\neg\sigma(\overline{m_e})$.

برهان. **(۱)** فرض کنید $\mathbf{T}\vdash\sigma(\overline{m_e})$. آنگاه از تعریف $\sigma(v_\circ)$ داریم

$$\sigma(\overline{m_e})\longleftrightarrow\mu\text{-unDef}_{\mathbf{T}}\text{-Lh}(\overline{m_e},|\sigma(\overline{m_e})|)$$

و بنابه توضیحات آمده در قسمت بالا $|\sigma(\overline{m_e})|=e$، پس μ-unDef$_{\mathbf{T}}$-Lh$(\overline{m_e},\overline{e})$ برقرار و در $\mathbf{T}$ اثبات‌پذیر است. از طرفی $\mu\text{-unDef}_{\mathbf{T}}\text{-Lh}(\overline{m_e},\overline{e})=\neg\mathsf{Def}_{\mathbf{T}}\text{-Lh}(\overline{m_e},\overline{e})\wedge\forall z<\overline{m_e}\,\mathsf{Def}_{\mathbf{T}}\text{-Lh}(z,\overline{e})$

بنابراین $\neg\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m_e},\overline{e})$ در $\mathbf{T}$ اثبات‌پذیر است. و بنابه تعریف ۹.۰.۲،

$$\sigma(\overline{m_e}) \wedge \forall v_{\circ}\forall v_{۱}\big(\sigma(v_{\circ}) \wedge \sigma(v_{۱}) \longrightarrow v_{\circ} = v_{۱}\big)$$

نیز در $\mathbf{T}$ قابل اثبات است. همچنین $\nu(\ulcorner\sigma(v_{\circ})\urcorner,\overline{m_e})$ عدد گودل جمله

$$\sigma(\overline{m_e}) \wedge \forall v_{\circ}\forall v_{۱}\big(\sigma(v_{\circ}) \wedge \sigma(v_{۱}) \longrightarrow v_{\circ} = v_{۱}\big)$$

می‌باشد؛ لذا طبق شرایط اثبات‌پذیری، $\mathbf{T} \vdash \mathsf{Pr}_T(\nu(\ulcorner\sigma(v_{\circ})\urcorner,\overline{m_e}))$. و بنابه تعریف $\mathsf{Fml}\text{-}\mathsf{Lh}(x,y)$، $\mathsf{Fml}\text{-}\mathsf{Lh}(\ulcorner\sigma(v_{\circ})\urcorner,\overline{e})$، یک Σ_1 جمله درست است، پس بنابر Σ_1 تمامیت $\mathbf{T}$، $\mathsf{Fml}\text{-}\mathsf{Lh}(\ulcorner\sigma(v_{\circ})\urcorner,\overline{e})$ قضیه‌ای از $\mathbf{T}$ است. بنابراین جمله $\exists z\Big(\mathsf{Pr}_T\big(\nu(z,\overline{m_e}) \wedge \mathsf{Fml}\text{-}\mathsf{Lh}(z,\overline{e})\big)\Big)$ در $\mathbf{T}$ اثبات‌پذیر است. پس $\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m_e},\overline{e})$ نیز در $\mathbf{T}$ اثبات‌پذیر است. در نتیجه $\mathbf{T}$ ناسازگار است؛ تناقض!

(۲) فرض کنید $\mathbf{T}$، Σ_1 درست باشد و $\mathbf{T} \vdash \neg\sigma(\overline{m_e})$. جمله $\neg\sigma(\overline{m_e})$ معادل جمله

$$\forall z < \overline{m_e}\ \Big(\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,\overline{e})\Big) \longrightarrow \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m_e},\overline{e})$$

است، زیرا

$$.\neg\sigma(\overline{m_e}) \longleftrightarrow \neg\mu\text{-}\mathsf{unDef}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m_e},\overline{e})$$

و از طرفی بنابه تعریف $\mu\text{-}\mathsf{unDef}_{\mathbf{T}}\text{-}\mathsf{Lh}(x,y)$ داریم

$$\begin{aligned}\neg\mu\text{-}\mathsf{unDef}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m_e},\overline{e}) &\equiv \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m_e},\overline{e}) \vee \exists z < \overline{m_e}\ \big(\neg\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,\overline{e})\big)\\ &\equiv \forall z < \overline{m_e}\ \Big(\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,\overline{e})\Big) \longrightarrow \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m_e},\overline{e})\end{aligned}$$

چون $\forall z < \overline{m_e}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,\overline{e})$ قابل اثبات در $\mathbf{T}$ است، آنگاه $\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m_e},\overline{e})$ در $\mathbf{T}$ اثبات‌پذیر است ولی $\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m_e},\overline{e})$ جمله‌ای نادرست است. در نتیجه $\mathbf{T}$، Σ_1 درست نمی‌باشد و این متناقص با فرض است. □

نتیجه زیر (قضیه اول ناتمامیت) در مقاله کیکوچی [۱۰] آمده است.

نتیجه ۱۲.۰.۲. *(۱) اگر $\mathbf{T}$ سازگار باشد، آنگاه* $\mathbf{T} \nvdash \neg\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m_e}, \overline{e})$؛
(۲) اگر $\mathbf{T}$، Σ_1 درست باشد، آنگاه $\mathbf{T} \nvdash \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m_e}, \overline{e})$.

برهان. **(۱)** فرض کنید $\mathbf{T} \vdash \neg\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m_e}, \overline{e})$. از طرفی، $\forall z < \overline{m_e}\, \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z, \overline{e})$ نیز در $\mathbf{T}$ اثبات‌پذیر است؛ بنابراین $\mathbf{T} \vdash \sigma(\overline{m_e})$. درنتیجه

$$\sigma(\overline{m_e}) \wedge \forall v_\circ \forall v_۱ \big(\sigma(v_\circ) \wedge \sigma(v_۱) \longrightarrow v_\circ = v_۱\big)$$

در $\mathbf{T}$ اثبات‌پذیر است؛ پس بنابه قسمت اول قضیه ۴.۰.۱ داریم $\mathbf{T} \vdash \mathsf{Pr}_{\mathbf{T}}(\nu(\ulcorner\sigma(v_\circ)\urcorner, \overline{m_e}))$. چون $\mathsf{Fml}\text{-}\mathsf{Lh}(\ulcorner\sigma(v_\circ)\urcorner, \overline{e})$، یک Σ_1 جمله درست است، بنابر Σ_1 تمامیت $\mathbf{T}$، $\mathsf{Fml}\text{-}\mathsf{Lh}(\ulcorner\sigma(v_\circ)\urcorner, \overline{e})$ قضیه‌ای از $\mathbf{T}$ است. بنابراین جمله $\exists z\Big(\mathsf{Pr}_{\mathbf{T}}\big(\nu(z, \overline{m_e}) \wedge \mathsf{Fml}\text{-}\mathsf{Lh}(z, \overline{e})\big)\Big)$ در $\mathbf{T}$ اثبات‌پذیر است. پس $\mathbf{T} \vdash \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m_e}, \overline{e})$، در نتیجه $\mathbf{T}$ ناسازگار است؛ تناقض!
(۲) فرض کنید $\mathbf{T}$، Σ_1 درست باشد و $\mathbf{T} \vdash \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m_e}, \overline{e})$. بنابه انتخاب عدد m_e و تعریف $\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(x, y)$، $\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m_e}, \overline{e})$ یک $\Sigma_۱$ فرمول نادرست است و $\mathbf{T} \vdash \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m_e}, \overline{e})$. بنابراین نظریه $\mathbf{T}$، $\Sigma_۱$ نادرست است و این تناقض است. □

حال، یک برهان جدید از قضیه ناتمامیت دوم بدون استفاده از نظریه مدل ارایه می‌دهیم.

تعریف ۱۳.۰.۲. برای هر $k \in \mathbb{N}$، فرض کنید n_k تعداد فرمول‌های با طول برابر یا کمتر از k باشد به طوری که متغیرهای آنها مابین $v_\circ, v_۱, \cdots, v_{k-۱}$ باشند.

لم ۱۴.۰.۲. *برای هر* $k \in \mathbb{N}$، $\mathbf{T} \vdash \mathsf{Con}(\mathbf{T}) \longrightarrow \exists z \leqslant \overline{n_k}\, \neg\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z, \overline{k})$.

برهان. بنابه تعریف $\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(x, y)$، فرمول زیر

$$\exists x_\circ \cdots \exists x_{n_k}\Big[\mathsf{Pr}_{\mathbf{T}}(v(x_\circ, \overline{0})) \wedge \cdots \wedge \mathsf{Pr}_{\mathbf{T}}(v(x_{n_k}, \overline{n_k})) \wedge \mathsf{Fml}\text{-}\mathsf{Lh}(x_\circ, \overline{k}) \wedge \cdots \wedge \mathsf{Fml}\text{-}\mathsf{Lh}(x_{n_k}, \overline{k})\Big]$$

در $\mathbf{T}+\forall z\leqslant\overline{n_k}\,\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,\overline{k})$ اثبات‌پذیر است. پس با استفاده از اصل لانه کبوتر اعداد متمایز $i,j<n_k$ وجود دارند به طوری که:

$$\mathbf{T}+\forall z\leqslant\overline{n_k}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,\overline{k})\vdash\exists x_i\Big(\mathsf{Pr}_{\mathbf{T}}\big(\nu(x_i,\bar{i})\big)\wedge\mathsf{Pr}_{\mathbf{T}}\big(\nu(x_i,\bar{j})\big)\Big).$$

چون $\mathsf{Pr}_{\mathbf{T}}(x)$، در قاعده وضع مقدم صدق می‌کند، پس فرمول زیر

$$\forall x\Big(\mathsf{Pr}_{\mathbf{T}}(\nu(x,\bar{i}))\wedge\mathsf{Pr}_{\mathbf{T}}(\nu(x,\bar{j}))\longrightarrow\mathsf{Pr}_{\mathbf{T}}(\ulcorner\bar{i}=\bar{j}\urcorner)\Big)$$

در $\mathbf{T}$ اثبات‌پذیر است. در نتیجه $\mathsf{Pr}_{\mathbf{T}}(\ulcorner\bar{i}=\bar{j}\urcorner)$ در $\mathbf{T}+\forall z\leqslant\overline{n_k}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,\overline{k})$ اثبات‌پذیر است. از طرف دیگر، جمله $\mathsf{Con}(\mathbf{T})\longrightarrow\neg\mathsf{Pr}_{\mathbf{T}}(\ulcorner\bar{i}=\bar{j}\urcorner)$ در T قابل اثبات است زیرا i و j مجزا هستند. بنابراین $\mathbf{T}+\forall z\leqslant\overline{n_k}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,\overline{k})+\mathsf{Con}(\mathbf{T})$ ناسازگار است. پس نتیجه می‌گیریم که
$\mathbf{T}\vdash\mathsf{Con}(\mathbf{T})\longrightarrow\exists z\leqslant\overline{n_k}\,\neg\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,\overline{k})$. □

لم ۱۵.۰.۲. *فرض کنید $m\in\mathbb{N}$. اگر $\mathbf{T}+\forall z\leqslant\overline{m}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,\overline{e})$ ناسازگار باشد، آنگاه $\mathbf{T}+\forall z<\overline{m}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,\overline{e})$ ناسازگار است.*

برهان. فرض کنید $\mathbf{T}+\forall z\leqslant\overline{m}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,\overline{e})$ ناسازگار باشد. آنگاه جمله

$$\neg\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m},\overline{e})\wedge\forall z<\overline{m}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,\overline{e})$$

یعنی $\sigma(\overline{m})$ اثبات‌پذیر در $\mathbf{T}+\forall z<\overline{m}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,\overline{e})$ است. چون

$$\sigma(\overline{m})\wedge\forall v_0\forall v_1\big(\sigma(v_0)\wedge\sigma(v_1)\longrightarrow v_0=v_1\big)$$

(بنابه تعریف $\sigma(x)$) نیز در $\mathbf{T}+\forall z<\overline{m}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,\overline{e})$ اثبات‌پذیر است، پس

$$\mathbf{T}\vdash\forall z<\overline{m}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z,\overline{e})\longrightarrow\sigma(\overline{m})\wedge\forall v_0\forall v_1\big(\sigma(v_0)\wedge\sigma(v_1)\longrightarrow v_0=v_1\big).$$

بنابه شرایط اثبات‌پذیری داریم

$$.\mathbf{T} \vdash \mathsf{Pr}_{\mathbf{T}}\big(\ulcorner \forall z < \overline{m}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z, \overline{e}) \urcorner\big) \longrightarrow \mathsf{Pr}_{\mathbf{T}}\big(\nu(\ulcorner \sigma(v_\circ) \urcorner, \overline{m})\big)$$

علاوه بر این، چون جمله $\forall z < \overline{m}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z, \overline{e})$ معادل یک Σ_1 جمله است، بنابه Σ_1 تمامیت صوری شده داریم:

$$\mathbf{T} \vdash \forall z < \overline{m}\, \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z, \overline{e}) \longrightarrow \mathsf{Pr}_{\mathbf{T}}\big(\ulcorner \forall z < \overline{m}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z, \overline{e}) \urcorner\big)$$

پس

$$.\mathbf{T} \vdash \forall z < \overline{m}\, \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z, \overline{e}) \longrightarrow \mathsf{Pr}_{\mathbf{T}}\big(v(\ulcorner \sigma(v_\circ) \urcorner, \overline{m})\big)$$

اما چون $\mathbf{T} \vdash \mathsf{Fml}\text{-}\mathsf{Lh}(\ulcorner \sigma(v_\circ) \urcorner, \overline{e})$ برقرار است پس

$$.\mathbf{T} \vdash \forall z < \overline{m}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z, \overline{e}) \longrightarrow \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m}, \overline{e})$$

بنابراین نظریه $\mathbf{T} + \forall z < \overline{m}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z, \overline{e})$ ناسازگار است زیرا این نظریه، هر دو جمله متناقض $\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m}, \overline{e})$ و $\neg\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{m}, \overline{e})$ را ثابت می‌کند. □

لم ۱۶.۰.۲. *اگر $\mathbf{T}$ سازگار باشد، آنگاه برای هر* $m \in \mathbb{N}$، $\mathbf{T} \nvdash \exists z \leqslant \overline{m}\, \neg\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z, \overline{e})$.

برهان. با استقراء روی m، لم را اثبات می‌کنیم. پایه استقراء بنابه لم ۱۵.۰.۲ بدیهی است. برای مرحله استقراء، فرض کنید که $\exists z < \overline{m}\ \neg\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z, \overline{e})$ در $\mathbf{T}$ اثبات‌پذیر باشد. اگر

$$\mathbf{T} + \forall z < \overline{m}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z, \overline{e})$$

ناسازگار باشد، آنگاه $\mathbf{T}$ ناسازگار است. بنابه لم ۱۵.۰.۲ اگر $\mathbf{T} + \forall z \leqslant \overline{m}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z, \overline{e})$ ناسازگار باشد، آنگاه $\mathbf{T} + \forall z < \overline{m}\ \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z, \overline{e})$ نیز ناسازگار است، بنابراین $\mathbf{T}$ ناسازگار است. □

قضیه ۲.۰.۱۷. (*قضیه ناتمامیت دوم*) *اگر* $\mathbf{T}$ *سازگار باشد، آنگاه* $\mathbf{T} \nvdash \mathsf{Con}(\mathbf{T})$.

برهان. اگر $\mathbf{T} \vdash \mathsf{Con}(\mathbf{T})$ ، آنگاه بنابه لم ۲.۰.۱۴ ، فرمول $\exists z \leqslant \overline{n_e}\ \neg \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(z, \overline{e})$ نیز اثبات‌پذیر است. پس بنابه لم ۲.۰.۱۶ ، $\mathbf{T}$ ناسازگار است؛ تناقض! $\square$

فصل ۳

پیچیدگی کولموگروف توسط اثبات‌پذیری در حساب

شایتین در مقاله [۵] قضیه ناتمامیت اول را بوسیله صوری‌سازی پارادوکس بری با استفاده از پیچیدگی کولموگروف اثبات کرد. در این فصل، نشان می‌دهیم برهان قضیه ناتمامیت توسط کیکوچی در مقاله [۱۰] که اصلاحی از برهان بولوس در مقاله [۳] است، گونه‌ای دیگر از برهان شایتین می‌باشد. به نظر می‌رسد که این استدلال را نمی‌توان در برهان اصلی بولوس صریحاً بکار برد، بنابراین می‌توانیم بگوییم برهان بولوس در اصل متفاوت از برهان شایتین است.

تعریف ۱۸.۰.۳. یک زبان برنامه‌نویسی تعیین می‌کنیم. پیچیدگی کولموگروف را برای $n \in \mathbb{N}$ طول کوتاهترین برنامه‌ای که خروجی‌اش n است تعریف می‌کنیم و با $K(n)$ نشان می‌دهیم.

به عبارت دقیق‌تر، پیچیدگی کولموگروف یک اندازه‌گیری از اطلاعات شامل دریک شئ متناهی است. قضیه زیر یک بازخوانی از قضیه ناتمامیت اول ثابت شده توسط شایتین است.

قضیه ۱۹.۰.۳. (*شایتین [۵]*) *اگر* $\mathbf{T}$ *درست باشد، آنگاه* $e \in \mathbb{N}$ *وجود دارد به طوری که برای همه اعداد طبیعی* n*، جمله* $e < K(n)$ *در* $\mathbf{T}$ *اثبات‌پذیر نیست.*

توجه کنید تعداد نامتناهی $n \in \mathbb{N}$ وجود دارد که $e < K(n)$ را ارضا می‌کند. بنابراین تعداد نامتناهی جملات درست اما اثبات‌ناپذیر وجود دارد. تعریف پیچیدگی کولوموگروف بستگی به انتخاب نوع زبان برنامه‌نویسی که از آن استفاده می‌کنیم دارد و این انتخاب می‌تواند تفسیری از یک ماشین تورینگ جهانی باشد. به طور کلی صحبت از یک ماشین تورینگ جهانی $S(z,x)$ (که z کد یک برنامه، x ورودی و $S(z,x)$ خروجی برنامه است) در اصطلاح، ساختنِ یک محمول بازگشتی ابتدایی $\mathscr{T}(z,x,y)$ و تابع بازگشتی ابتدایی $\mathscr{U}(y)$ است. $\mathscr{T}(z,x,y)$ که به عنوان محمول کلینی[۱] شناخته شده بدین معنی است که y کد محاسبه از یک برنامه با کد z روی ورودی x است. اگر y کد یک محاسبه باشد خروجی‌اش $\mathscr{U}(y)$ است و $S(z,x) \simeq \mathscr{U}\left(\mu y[\mathscr{T}(z,x,y)]\right)$.

تعریف ۲۰.۰.۳. تابع بازگشتی $S(z,x)$ را یک ماشین تورینگ جهانی گوییم اگر یک رابطه بازگشتی ابتدایی $\mathscr{T}(z,x,y)$ و یک تابع بازگشتی ابتدایی $\mathscr{U}(y)$ وجود داشته باشد به طوری که

$$S(z,x) \simeq \mathscr{U}\left(\mu y[\mathscr{T}(z,x,y)]\right)$$

[۱] Kleene

و S شرایط زیر را ارضاء کند:

(۱) برای هر توابع بازگشتی $f(x)$ یک برنامه با کد $e \in \mathbb{N}$ وجود دارد به طوری که

$$.f(x) \simeq S(e,x)$$

(۲) برای هر $e \in \mathbb{N}$ یک تابع بازگشتی $f(x)$ وجود دارد به طوری که

$$.f(x) \simeq S(e,x)$$

ملاحظه می‌کنیم که هرگاه یک زبان برنامه نویسی داشته باشیم چنین $\mathscr{T}$ و $\mathscr{U}$ را می‌توان تعریف کرد. برعکس، اگر چنین $\mathscr{T}$ و $\mathscr{U}$ که شرایط تعریف بالا را ارضاء می‌کند وجود داشته باشند، می‌توانیم بگوییم که یک زبان برنامه نویسی در دسترس داریم. برای یک ماشین تورینگ جهانی $S(z,x)$، تعریف می‌کنیم $K(x) = \mu z[S(z,0) = x]$ بنابراین تابع $K(x)$، نوعی ویژگی با پیچیدگی کولوموگروف تعریف شده در طول برنامه را به نمایان می‌کند. بنابراین می‌توانیم $K(x)$ را به عنوان یک پیچیدگی کولموگروف در نظر بگیریم. اگر چه مفهوم طول یک برنامه به صراحت در این تعریف معلوم نیست. باید پیچیدگی کولوموگروف در این معنا را با مراجعه به اثبات‌پذیری در حساب در نظر بگیریم.

تعریف ۲۱.۰.۳. برای هر نظریه بازگشتی $\mathbf{T}$ از حساب، یک محمول بازگشتی ابتدایی $\mathscr{T}_{\mathbf{T}}(z,x,y)$ و یک تابع بازگشتی ابتدایی $\mathscr{U}_{\mathbf{T}}(y)$ به شرح زیر تعریف می‌کنیم.

(۱) $\mathscr{T}_{\mathbf{T}}(i,m,p)$ برقرار است اگر وتنها اگر $i = \ulcorner\varphi(v_0,v_1)\urcorner$، و p عدد گودل یک برهان برای جمله $\varphi(\overline{m},\overline{n}) \wedge \forall v_0 \forall v_1 \big(\varphi(\overline{m},v_0) \wedge \varphi(\overline{m},v_1) \longrightarrow v_0 = v_1\big)$ از نظریه $\mathbf{T}$ به ازای یک عدد $n < p$ باشد.

(۲) $n = \mathscr{U}_{\mathbf{T}}(p)$ اگر p عدد گودل یک برهان در نظریه $\mathbf{T}$ از جمله

$$\varphi(\overline{m},\overline{n}) \wedge \forall v_0 \forall v_1 \big(\varphi(\overline{m},v_0) \wedge \varphi(\overline{m},v_1) \longrightarrow v_0 = v_1\big)$$

برای یک عدد $m < p$ بوده و $\varphi(v_\circ)$ فرمولی با عدد گودل کمتر از p باشد.

به عبارت دیگرفرمول‌هایی را که اعداد را نام‌گذاری می‌کنند، به عنوان برنامه‌هایی در نظر می‌گیریم که خروجی‌هایشان اعداد نام‌گذاری شده می‌باشند؛ و ما می‌توانیم برهان‌های صوری این جملات خاص را به عنوان محاسبات برنامه‌های تعیین شده با این فرمول‌ها در نظر بگیریم.

لم ۲۲.۰.۳. *تعریف کنید* $S_{\mathbf{T}}(z,x) \simeq \mathscr{U}_{\mathbf{T}}\big((\mu y)[\mathscr{T}_{\mathbf{T}}(z,x,y)]\big)$. *تابع* $S_{\mathbf{T}}(z,x)$ *یک ماشین تورینگ جهانی است.*

برهان. شرایط تعریف ۲۰.۰.۳ را بررسی می‌کنیم. برای قسمت اول، بنابه گزاره ۶.۰.۱ برای هر تابع بازگشتی $f(x)$ یک فرمول $\varphi(x,y)$ وجود دارد که نمایانگر $f(x)$ است. اگر $f(m)\uparrow$ آنگاه برای هر $n \in \mathbb{N}$، $\mathbf{T} \nvdash \varphi(\overline{m},\overline{n})$ بنابراین $\mathscr{T}_{\mathbf{T}}\big(\ulcorner\varphi(v_\circ,v_1)\urcorner,m,p\big)$ برای هیچ $p \in \mathbb{N}$ برقرار نیست. فرض کنید $f(m)=n$، و p کوچکترین عدد گودل برای برهانی از

$$\varphi(\overline{m},\overline{n}) \wedge \forall v_\circ \forall v_1 \big(\varphi(\overline{m},v_\circ) \wedge \varphi(\overline{m},v_1) \longrightarrow v_\circ = v_1\big)$$

در $\mathbf{T}$ باشد. آنگاه $\mathscr{T}_{\mathbf{T}}\big(\ulcorner\varphi(v_\circ,v_1)\urcorner,m,p\big)$ برقرار است و $\mathscr{U}_{\mathbf{T}}(p)=n$. بنابراین

$$S_{\mathbf{T}}\big(\ulcorner\varphi(v_\circ,v_1)\urcorner,m\big) = n.$$

از این رو $f(x) \simeq S_{\mathbf{T}}\big(\ulcorner\varphi(v_\circ,v_1)\urcorner,x\big)$. و برای قسمت دوم ، اگر e عدد گودل فرمول $\varphi(v_\circ,v_1)$ باشد و برای m و n، $\varphi(\overline{m},\overline{n}) \wedge \forall v_\circ \forall v_1 \big(\varphi(\overline{m},v_\circ) \wedge \varphi(\overline{m},v_1) \longrightarrow v_\circ = v_1\big)$ برقرار باشد، آنگاه یک تابع f با دامنه $\mathbb{N}$ وجود دارد به طوری که $f(x) \simeq S_T(e,x)$. چون $\varphi(v_\circ,v_1)$ نمایانگر f بوده و بنابه گزاره ۶.۰.۱، f تابع بازگشتی است، در نتیجه $S_{\mathbf{T}}(z,x)$ یک ماشین تورینگ جهانی است. □

بنابراین می‌توانیم پیچیدگی کولموگروف توسط ماشین تورینگ جهانی $S_{\mathbf{T}}(z,x)$ را تعریف کنیم.

تعریف ۲۳.۰.۳. فرض کنید n یک عدد طبیعی باشد. پیچیدگی کولوموگروف برای n در $\mathbf{T}$، را

برابر طول کوتاهترین فرمول $\varphi(v_0, v_1)$ به طوری که $S_{\mathbf{T}}(\ulcorner\varphi(v_0,v_1)\urcorner, 0) = n$ تعریف می‌کنیم و با $K_{\mathbf{T}}(n)$ نمایش می‌دهیم.

واضح است که $K_{\mathbf{T}}(x)$ با توجه به تعریف ۹.۰.۲ کوتاهترین طول از یک فرمول است که n را توصیف می‌کند. رُی[۲] در مقاله [۱۰] مستقیماً تابع $K_{\mathbf{T}}(x)$ را تعریف کرده و اثبات کرد که $K_{\mathbf{T}}(x)$ بازگشتی نیست. به دنبال این نتیجه، روشن می‌شود که $K_{\mathbf{T}}(x)$ شکلی از پیچیدگی کولوموگروف است (مرجع [۲۲] را ببینید). در حقیقت می‌توانیم رابطه $y < K_{\mathbf{T}}(x)$ را توسط فرمول $\neg\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(x,y)$ بیان کنیم. حال لم ۱۶.۰.۲ را بازنویسی می‌کنیم.

قضیه ۲۴.۰.۳. *اگر $\mathbf{T}$ سازگار باشد آنگاه $e \in \mathbb{N}$ وجود دارد به طوری که برای هر $m \in \mathbb{N}$،* $\mathbf{T} \nvdash e < K_T(m)$.

در حالی که شرایط قضایای ۱۹.۰.۳ و ۲۴.۰.۳ کمی متفاوت از هم هستند، قضیه ۲۴.۰.۳ مشابه قضیه ۱۹.۰.۳ است. نتیجه‌ای از قضیه ناتمامیت در مقاله کیکوچی [۱۰]، نوعی ضیف از لم ۱۶.۰.۲ است، و می‌توانیم بگوییم نوعی ضعیف تر از حالت خاصی از قضیه ۱۹.۰.۳ است که توسط تعیین کردن یک ماشین تورینگ خاص مشاهده می‌شود. تا جایی که می‌توانیم، درباره این پیچیدگی کولوموگروف خاص $K_{\mathbf{T}}(x)$ مبتنی بر ماشین تورینگ جهانی $S_{\mathbf{T}}(z,x)$، یک نوع قوی از قضیه ۲۴.۰.۳ را اثبات کنیم.

قضیه ۲۵.۰.۳. *فرض کنید* $p = min\{|\varphi| : \text{یک فرمول است } \varphi\}$. *اگر $\mathbf{T}$ سازگار باشد، آنگاه برای هر $n \in \mathbb{N}$ و برای هر عدد طبیعی* $m \geq p$، $\mathbf{T} \nvdash m < K_{\mathbf{T}}(n)$.

برهان. فرض کنید φ یک فرمول با طول p و m، n اعداد طبیعی با شرط $m \geq p$ بوده و $\mathbf{T}$ سازگار باشد. آنگاه بنابه Σ_1 تمامیت، $\mathsf{Fml}\text{-}\mathsf{Lh}(\ulcorner\varphi\urcorner, \overline{m})$ در $\mathbf{T}$ قابل اثبات است. چون این مطلب که «اگر $\mathbf{T}$ سازگار باشد آنگاه ψ در $\mathbf{T}$ اثبات‌پذیر است» در $\mathbf{T}$ قابل صوری سازی است، برای هر فرمول φ، داریم:

$$\mathbf{T} \vdash \neg\mathsf{Con}(\mathbf{T}) \longrightarrow \mathsf{Pr}_{\mathbf{T}}(\nu(\ulcorner\varphi\urcorner, \overline{\mathsf{n}}))$$

[۲] Roy

از این رو بدست می‌آوریم $\mathbf{T} \vdash \neg\mathsf{Con}(\mathbf{T}) \rightarrow \mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{n}, \overline{m})$، بنابراین

$$\mathbf{T} \vdash \neg\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{n}, \overline{m}) \rightarrow \mathsf{Con}(\mathbf{T}).$$

و بالاخره بنابه قضیه دوم ناتمامیت فرمول $\neg\mathsf{Def}_{\mathbf{T}}\text{-}\mathsf{Lh}(\overline{n}, \overline{m})$ یعنی $m < K_{\mathbf{T}}(n)$ در $\mathbf{T}$ اثبات‌ناپذیر است. $\square$

فصل ۴

پیچیدگی کولموگروف و ثوابت مشخصه‌ی نظریه‌های صوری حساب

ماشین‌های تورینگ در PA

تعریف ۲۶.۰.۴. مجموعه S از فرمول‌ها را در زبان L شمارای کارآمد گویند هرگاه الگوریتمی (متناهی) وجود داشته باشد که بتواند همه‌ی عناصر S را به عنوان خروجی فهرست کند.

حال، فرمولی را معرفی می‌کنیم که حرکت‌های ماشین‌های تورینگ را توصیف می‌کند.

یک Δ_0 فرمول $\Psi_0(x,y)$ موجود است به طوری که $\mathbb{N} \models \Psi_0(p,m)$ اگر و فقط اگر عدد p یک پردازش از ماشین تورینگی که توسط عدد m رمزنگاری شده است را نشان دهد. به منظور توصیف تابع ارایه شده توسط یک ماشین تورینگ، ما باید توسط یک فرمول منطقی ارتباط بین یک عدد طبیعی و رشته‌ی دودویی متناظر آن را توصیف کنیم. عبارات زیر معادلند:

- $x = a_0 2^n + a_1 2^{n-1} + ... + a_{n-1} 2 + a_n$
- دنباله $x_0, x_1, ..., x_n$ موجود است به طوری که $x_0 = a_0$، $x_i = 2x_{i-1} + a_i$ برای $i = 1, ..., n$ و $x = x_n$.

بنابراین، Σ_1 فرمول $\mathsf{bin}(x,t)$ موجود است که می‌گوید «t عدد دنباله‌ای است که نمایش دودویی از x را رمزنگاری می‌کند». بنابراین یک Σ_1 فرمول مانند $\Psi_1(m,y,z)$ داریم که بیان می‌کند «z یک ID از ماشین تورینگی است که با m کدگزاری شده و محتویات نوار، نمایش دودویی از عدد y است». با استفاده از این فرمول، یک Σ_1 فرمول $\Psi_2(p,m,x)$ را می‌توان تعریف کرد که بیان می‌کند «p عددی است که یک دنباله معتبر از ID ماشین تورینگ کد شده با m توسط نمایش دودویی از x در نوار را در شروع نمایش می‌دهد». فرض کنید Φ_m ماشین تورینگ کد شده توسط m باشد و آن را با یک تابع محاسبه‌پذیر (جزئی) تعریف شده توسط Φ_m شناسایی کنید. پس عبارت «$\Phi_m(x) = y$» یا «$\Phi_m(x) \downarrow y$» را می‌توان به صورت زیر نوشت

$$\exists p \big[\Psi_0(p,m) \wedge \exists n, t_0, t_2, i < p \; (n = |p| \wedge p[0] = \langle I_M, t_1, 0 \rangle \\ \wedge p[n] = \langle q, t_2, 0 \rangle \text{ for some } q \in F_m \wedge \mathsf{bin}(x,t_1) \wedge \mathsf{bin}(y,t_2)) \big].$$

تعریف ۲۷.۰.۴. فرض کنید f یک تابع دوسویی Σ_1 تعریف‌پذیر در PA باشد. $\mathsf{CT}(d,m)$ را فرمولی در نظر بگیرید که بیان می‌کند d کد یک ID است که پایان متعارفی از m را ارایه می‌دهد و $\mathsf{tval}(d,x)$ فرمولی باشد که بیان می‌کند d کد یک ID است با نواری که مقدار آن توسط x نمایش داده می‌شود. ما $\Phi_m^f(x)\downarrow y$ را به جای فرمول

$$\exists p\big[\Psi_2(p,f(m),x)\wedge\exists l(|p|=l\wedge\mathsf{CT}(p[l],m)\wedge\mathsf{tval}(p[l],y))\big]$$

می‌نویسیم. اگر محاسبه‌ی Φ_m^f متعارفاً پایان نپذیرد آن را با $\Phi_m^f\uparrow$ نشان می‌دهیم که معادل است با

$$.\forall p\big[\Psi_2(p,f(m),x)\longrightarrow\neg\exists l(|p|=l\wedge\mathsf{CT}(p[l],m)\wedge\mathsf{tval}(p[l],y))\big]$$

برای عدد طبیعی n، پیچیدگی کولموگروف n نسبت به f را با $K^f(n)$ نمایش می‌دهیم که کوچک‌ترین عدد طبیعی kای است که تساوی $\Phi_k^f=n$ برقرار باشد. می‌توانیم $K^f(x)=y$ را با «y کوچک‌ترین mای است که داشته باشیم $\exists p\Psi_2(p,f(m),0,x)$» تعریف کنیم.

تعریف ۲۸.۰.۴. $\mathbf{T}$ را یک سیستم صوری در نظر بگیرید که توسیع PA است. دو ثابت مشخصه $c_{f,\mathbf{T}}$ و $r_{f,\mathbf{T}}$ را به صورت زیر تعریف می‌کنیم:

$c_{f,\mathbf{T}}$ کوچک‌ترین kای است که برای هر عدد طبیعی n، داشته باشیم $\mathbf{T}\nvdash K^f(n)>k$.

$r_{f,\mathbf{T}}$ کوچک‌ترین eای است به طوری که داشته باشیم $\Phi_e^f\uparrow$ و $\mathbf{T}\nvdash\Phi_e^f\uparrow$.

تعریف ۲۹.۰.۴. فرض کنید M یک ماشین تورینگ باشد و l را یک عدد طبیعی در نظر بگیرید.

(۱) M^l ماشین تورینگی است که به صورت زیر تعریف می‌کنیم: حالت‌های M^l را همان حالت‌های M بعلاوه‌ی حالت جدید q_f در نظر بگیرید به طوری که q_f تنها حالت نهایی M^l می‌باشد. دستورات M^l همان دستورات M به اضافه‌ی دستورهایی باشد که به آن فرمان می‌دهد زمانی که کنترل M^l حالتی نهایی در F_M را وارد می‌کند، M^l نوار ارزش را l کند و با حالت q_f متوقف می‌شود.

(۲) $M^{(l)}$ به عنوان ماشین تورینگی که از اضافه کردن حالت جدید q_f و دستورهای جدید زیر به M به دست آمده تعریف شده است: اگر $M^{(l)}$ حالت نهایی از M را وارد کند، آنگاه مقدار خروجی نوار را بررسی کند؛ اگر خروجی l باشد $M^{(l)}$ مقدار نوار را $l+1$ کند در غیر این صورت $M^{(l)}$ هیچ کاری انجام ندهد. بنابراین $M^{(l)}$ ورودی q_f را وارد کرده و متوقف می‌شود.

لم ۳۰.۰.۴. *فرض کنید M ماشین تورینگ بدون ورودی بوده و l را یک عدد طبیعی در نظر بگیرید. در این صورت* PA *اثبات می‌کند:*

(۱) $(M \uparrow \longleftrightarrow M^l \uparrow) \wedge (M \uparrow \longleftrightarrow M^{(l)} \uparrow)$،

(۲) $M^l \downarrow \longrightarrow M^l \downarrow l$،

(۳) $M^{(l)} \not\downarrow l$،

(۴) $\forall x \neq l (M \downarrow x \longleftrightarrow M^{(l)} \downarrow x)$.

برهان. (۱) ما می‌توانیم برهان زیر را در PA فرموله کنیم. فرض کنید $M \uparrow$. ما یک پردازش طویل p از M داریم. می‌دانیم که، p پردازشی از M^l و بعضی وقت‌ها پردازشی از $M^{(l)}$ است. اگر M^l یا $M^{(l)}$ متوقف شوند آنگاه p توسیعی از یک پردازش پایان‌دار از M^l یا $M^{(l)}$ می‌باشد که یک تناقض است. بنابراین داریم

$$M \uparrow \longrightarrow M^l \uparrow \wedge M^{(l)} \uparrow.$$

فرض کنید که با پردازشی پایان‌دار مانند p داشته باشیم $M \downarrow$. می‌توانیم p را به پردازشی پایان‌دار از M^l با اضافه کردن بعضی حرکت‌های خاص توسیع دهیم به این نحو که چون p پردازشی پایان‌دار از M است لذا در حالت نهایی q'_f ای پایان پذیرفته و متوقف می‌شود؛ ما این q'_f را به کنترل M^l می‌دهیم که در این صورت طبق تعریف ۲۹.۰.۴، M^l با حالت نهایی q_f متوقف می‌شود پس $M^l \downarrow$. برای ارایه‌ی پردازشی پایان‌دار از $M^{(l)}$، به تغییر دستورات $M^{(l)}$ رجوع کرده و تمام پردازش‌های پایان‌دار ممکن از $M^{(l)}$ که p را توسیع می‌دهند را لیست می‌کنیم. بنابراین PA اثبات می‌کند که حداقل یکی پیدا می‌شود که توسط $M^{(l)}$ تحقق می‌یابد، به هر حال ما معلوم نمی‌کنیم کدام یک از آن نامزدها تحقق می‌یابد. بنابراین PA، $M \downarrow \longrightarrow M^l \downarrow \wedge M^{(l)} \downarrow$ را ثابت می‌کند.

(۲) فرض کنید که $M^l \downarrow$. ما پردازشی پایان‌دار از M^l داریم. از آنجایی که تنها حالت نهایی M^l، q_f است پس با توجّه به بند اوّل تعریف ۲۹.۰.۴، می‌بایست این پردازش با ID نهایی که حاوی حالت نهایی q_f و خروجی l است پایان یابد و این نتیجه می‌دهد که $M^l \downarrow l$.

(۳) این قسمت به وضوح از بند دوّم تعریف ۲۹.۰.۴ به دست می‌آید. زیرا اگر $M^{(l)}$ با حالت نهایی q'_f و خروجی l متوقف شود، طبق تعریف ۲۹.۰.۴، ماشین تورینگ پردازش‌های خود را ادامه

داده و با پردازشی نوار ارزش را $l+1$ کرده و با حالت نهایی q_f متوقف می‌شود. لذا هیچ گاه $M^{(l)} \downarrow l$.

(۴) فرض کنید که $l \neq x$ و $M \downarrow l$. ما پردازشی پایان‌دار مانند p از M با حالت نهایی q'_f ای داریم. با توجه به قسمت دوّم تعریف ۲۹.۰.۴، $M^{(l)}$ این حالت نهایی را وارد می‌کند و چون $l \neq x$ است هیچ کاری روی نوار انجام نداده و حالت نهایی q_f را وارد کرده و با همان ارزش نواری x متوقف می‌شود. پس $M^{(l)} \downarrow x$. برای عکس فرض کنید که $l \neq x$ و $M^{(l)} \downarrow x$. فرض (خلف) می‌کنیم که $M \not\downarrow x$. در این صورت یا $M \uparrow$ یا y ای وجود دارد که $x \neq y$ و $M \downarrow y$. حالت اوّل، $M \uparrow$، نمی‌تواند برقرار باشد زیرا با توجّه به اوّلین بند همین لم، می‌بایست $M^{(l)} \uparrow$ که متناقض با فرض است. حالت دوّم، $M \downarrow y$، نیز نمی‌تواند برقرار باشد. زیرا اگر $l \neq y$ باشد با توجه به روند اثبات قسمت رفت، $M^{(l)} \downarrow y$ که متناقض با $x \neq y$ است؛ و اگر $l = y$ باشد $M^{(l)} \downarrow l$ با سوّمین بند همین لم در تناقض است. $\square$

لم ۳۱.۰.۴. *برای هر Π_1 جمله φ، ماشین تورینگ D_φ موجود است به طوری که* PA*، $D_\varphi \uparrow \longleftrightarrow \varphi$ و $D_\varphi \downarrow 0 \longleftrightarrow \neg\varphi$ را ثابت می‌کند.*

برهان. ما می‌توانیم یک ماشین تورینگ مانند D_0 را طوری بسازیم که درستی مقادیر Δ_0 جمله‌ها را ارزیابی کند. با استفاده از D_0 ماشین تورینگ D_1 را به صورت زیر تعریف می‌کنیم: اگر برای برخی از Δ_0 فرمول‌های $\varphi(x)$، عدد گودل $\forall x\varphi(x)$، $\ulcorner\forall x\varphi(x)\urcorner$، را به عنوان ورودی به D_0 بدهیم، در این صورت D_1 درستی هر $\varphi(n)$ را با استفاده از D_0 یکی یکی برای $n = 0, 1, \ldots$ تعیین کند. اگر D_1 دریافت که برای بعضی n ها $\varphi(n)$ نادرست است، آنگاه D_1 متوقف شده و خروجی 0 را بدهد؛ در غیر این صورت D_1 مقدار n را افزایش دهد. برای هر Π_1 جمله‌ی τ، $D(\ulcorner\tau\urcorner)$ را به عنوان ماشین تورینگ بدون ورودی D_τ در نظر می‌گیریم. اگر φ را در PA فرض کنیم، با استقراء روی پردازش‌ها، پردازش به طور دلخواه طولانی از D_τ داریم. برای طرف دیگر، پردازش پایان‌دار p از D_φ متناظر با $\neg\varphi$ در PA تعریف‌پذیر است. با فرض این که $\neg\varphi$ در PA است، می‌توانیم اثبات کنیم که p پردازشی معتبر برای D_1 است و لذا داریم $D_1 \downarrow$. $\square$

لم ۳۲.۰.۴. *نظریه‌های $\mathbf{S}$ و $\mathbf{T}$ را در نظر بگیرید. در این صورت ماشین تورینگ $A_{\mathbf{S},\mathbf{T}}$ موجود است*

به طوری که $A_{\mathbf{S},\mathbf{T}}$ متوقف نمی‌شود و برای هر n، هیچ کدام از $\mathbf{S}$ و $\mathbf{T}$ نمی‌تواند ثابت کند $A_{\mathbf{S},\mathbf{T}}$ خروجی n را نمی‌دهد. در نتیجه هیچ یک از $\mathbf{S}$ و $\mathbf{T}$ نمی‌تواند عدم توقف $A_{\mathbf{S},\mathbf{T}}$ را ثابت کند.

برهان. با استفاده از قضیه بازگشت می‌توانیم ماشین تورینگ $A_{\mathbf{S},\mathbf{T}}$ را به دست بیاوریم به طوری که $A_{\mathbf{S},\mathbf{T}}$ یک برهان برای یک قضیه به شکل $A_{\mathbf{S},\mathbf{T}} \not\downarrow n$ را در هر یک از $\mathbf{S}$ و $\mathbf{T}$ جستجو کرده و اگر یافت n را به عنوان خروجی بدهد و متوقف شود. فرض کنید که برای بعضی m ها، $\mathbf{S}$ یا $\mathbf{T}$، $A_{\mathbf{S},\mathbf{T}} \not\downarrow m$ را اثبات کند. بنابراین عددی مانند n موجود است به طوری که $A_{\mathbf{S},\mathbf{T}} \downarrow n$ و یکی از $\mathbf{S}$ یا $\mathbf{T}$، $A_{\mathbf{S},\mathbf{T}} \not\downarrow n$ را ثابت می‌کند. اما هر دوی $\mathbf{S}$ و $\mathbf{T}$، $A_{\mathbf{S},\mathbf{T}} \downarrow n$ را زمانی ثابت می‌کنند که آن Σ_1 جمله‌ی درست باشد. که این متناقض با سازگاری $\mathbf{S}$ یا سازگاری $\mathbf{T}$ می‌باشد. □

ثوابت مشخصه

راتیکاینن استدلال کرد که $c_{\mathbf{T}}$ پیچیدگی $\mathbf{T}$ را نشان نمی‌دهد و ثابت کرد که $c_{\mathbf{T}}$ می‌تواند با انتخاب مناسب ماشین تورینگ جهانی صفر یا به طور دلخواه بزرگ ساخته شود که در ادامه تحت عنوان قضیه ۳۵.۰.۴ و قضیه ۳۶.۰.۴ بیان خواهیم کرد. وی مقدار دیگری را هم مطرح کرد که با $r_{\mathbf{T}}$ نشان داده و آن را نسبت به $\mathbf{T}$ و یک ماشین تورینگ جهانی در روشی مشابه $c_{\mathbf{T}}$ تعریف کرد.

قضیه ۳۳.۰.۴. *برای هر سیستم صوری صحیح و متناهیاً مشخص شده $\mathbf{T}$ و جایگشت تعریف‌پذیر f در PA، $c_{f,\mathbf{T}}$ و $r_{f,\mathbf{T}}$ موجودند.*

برهان. نشان می‌دهیم $c_{f,\mathbf{T}}$ موجود است یعنی عدد طبیعی c موجود است به طوری که $\mathbf{T} \nvdash K^f(x) > c$. تابع تام محاسبه‌پذیر i را به صورت زیر تعریف کنید: برای هر k، ماشین تورینگی داریم که برای تمامی xها برهان $K^f(x) > k$ را از $\mathbf{T}$ جستجو کرده و اگر پیدا کرد با خروجی x متوقف می‌شود. می‌توانیم به طور کارآمد، اندیس این ماشین را $i(k)$ در نظر بگیریم. با قضیه بازگشت، به طور کارآمد می‌توانیم اندیسی مانند c بیابیم به طوری که $\Phi_c \simeq \Phi_{i(c)}$. اگر برای عدد طبیعی x داشته باشیم $\mathbf{T} \vdash K^f(x) > c$، یعنی $\Phi_{i(c)} \simeq \Phi_c \downarrow x$، خواهیم داشت $K^f(x) \leq c$ که این متناقض با فرض صحت $\mathbf{T}$ است. حال نشان می‌دهیم که $r_{f,\mathbf{T}}$ موجود است. یک ماشین تورینگ مانند $\Phi_{i(k)}$ را در

نظر بگیرید به طوری که اگر $\mathbf{T} \vdash \Phi_k \uparrow$ آنگاه متوقف شود. با استفاده از قضیه بازگشت cای موجود است به طوری که $\Phi_{i(c)} \simeq \Phi_c$. Φ_c متوقف نمی‌شود چون اگر $\Phi_c \downarrow$ آنگاه $\Phi_{i(c)} \downarrow$ پس $\mathbf{T} \vdash \Phi_c \uparrow$ که با صحت $\mathbf{T}$ تناقض دارد، بنابراین $\Phi_c \uparrow$. اگر $\mathbf{T} \vdash \Phi_c \uparrow$، پس $\Phi_{i(c)}$ متوقف می‌شود، بنابراین، Φ_c متوقف می‌شود که تناقض است. پس داریم $\mathbf{T} \nvdash \Phi_c \uparrow$. □

تعریف ۳۴.۰.۴. فرض کنید $\mathbf{T}$ یک نظریه و Φ یک ماشین تورینگ جهانی باشد که متناظر با شمارشی بازگشتی از تمام ماشین‌های تورینگ بدون ورودی است.

۱. (PA) برای اعداد طبیعی x و y، پیچیدگی کولموگروف x، $K(x)$، کوچک‌ترین عدد طبیعی y ای است که $\Phi_y \downarrow x$.

۲. ثابت مشخصه $c_{\mathbf{T}}$ از $\mathbf{T}$، کوچک‌ترین y ای است که برای هر عدد طبیعی x، $\mathbf{T}$ هیچ قضیه ای به فرم $y < K(x)$ را ثابت نکند.

۳. $r^{\Phi}_{\mathbf{T}}$ کوچک‌ترین i ای است که Φ_i متوقف نمی‌شود و $\mathbf{T}$ نمی‌تواند عدم توقف آن را ثابت کند.

در قضیه ۳۳.۰.۴ نشان دادیم که $c_{\mathbf{T}}$ و $r_{\mathbf{T}}$ برای هر نظریه صوری $\mathbf{T}$ موجودند. ماشین تورینگ جهانی Φ را با نشان دادن K با K^{Φ}، $c_{\mathbf{T}}$ با $c^{\Phi}_{\mathbf{T}}$ و $r_{\mathbf{T}}$ با $r^{\Phi}_{\mathbf{T}}$ مشخص می‌کنیم.

قضیه ۳۵.۰.۴. *برای هر نظریه صوری $\mathbf{T}$ که توسیع PA باشد، ثابت مشخصه شایتین، $c_{\mathbf{T}}$، می‌تواند صفر باشد.*

برهان. فرض کنید که رمزنگاری دوسویی اوّلیه π از ماشین‌های تورینگ به اعداد طبیعی داده شده است و می توان آن‌ها را با Φ_0 و Φ_1 و ... شمارش کرد. تابع رمزگزین π^n (نسبت به عامل n داده شده) را به صورت زیر تعریف می‌کنیم:

$$\pi^n(x) = \begin{cases} 0 & x = n \\ x+1 & x < n \\ x & x > n. \end{cases}$$

واضح است که برای رمزنگاری اولیّه π و عدد n داده شده، می‌توان به طور کارآمد رمزنگاری جدید تعیین شده توسط π^n را به دست آورد. پیچیدگی کولموگروف را نسبت به این رمزنگاری جدید K^n می‌نامیم به طوری که $K^n(x) = \mu z(\exists y[\pi^n(y) = z \ \wedge\ \Phi_y \downarrow x])$. پیچیدگی کولموگروف حسابی است و می‌توان یک فرمول صوری که آن را (برای رمزنگاری اولیّه) تعریف می‌کند ساخت. برای این فرمول داده شده، زمانی می‌توان به طور کارآمد فرمولی که برای n داده شده K^n را تعریف می‌کند یافت که به سادگی با استفاده از صوری‌سازی تعریف فوق از π^n باشد. بعلاوه، برای عدد گودلِ فرمول قبلی داده شده، می‌توان به طور کارآمد عدد گودلِ فرمول اخیر را پیدا کرد. و زمانی می‌توان به طور کارآمد ماشین تورینگ Φ_m (که رمز آن از رمزنگاری اولیّه m است) یافت که حداقل xای را جستجو کند که برای بعضی pها ، $\mathsf{Prf}_{\mathbf{T}}(x, \ulcorner K^n(p) > 0 \urcorner)$؛ و زمانی که یافت (اگر چنین xای وجود داشته باشد) برای هر x که این را ثابت کند، p را چاپ کند. حال وقت آن است که ماشینی بیابیم که شبیه این عمل کرده و عدد رمز اولیّه‌اش را به عنوان عامل n در K^n داشته باشد. به طور غیر رسمی، ماشین مطلوب می‌توانست به صورت زیر تعریف شده باشد: از 0 شروع شود، برای هر عدد بررسی کند که آیا آن برای بعضی pها، (یک عدد گودلِ) برهانی از یک فرمول به شکل $K^e(p) > 0$ است یا نه. اگر چنین قضیه‌ای پیدا شد، عدد ویژه‌ی p که این حقیقت برای آن ثابت شده است را چاپ کند. با رسمیت بیشتر، این خودارجاع می‌تواند به صورت زیر دستکاری شده باشد: تابع بازگشتی $f(x)$ وجود دارد به طوری که برای عامل n داده شده در K^n، $f(n) = m$ عدد رمز (اولیّه) ماشین تورینگی که در بالا توصیف کردیم است. با استفاده از قضیه بازگشت، عدد eای وجود دارد به طوری که Φ_e و $\Phi_{f(e)}$ همان تابع را محاسبه می‌کنند. بعلاوه، برهان قضیه بازگشت بیان نمی‌کند که چنین عدد eای موجود است بلکه صریحاً آن را می‌سازد. بنابراین، می‌توان به طور کارآمد یک چنین eای یافت. به هر حال، ادامه می‌دهد که این برنامه هرگز متوقف نخواهد شد و در نتیجه برای هر p، نمی‌توان $K^e(p) > 0$ را ثابت کرد. اگر می‌توانست چنین قضیه‌ای را ثابت کند، برنامه e متوقف خواهد شد و عدد p را چاپ می‌کند که قضیه برای آن توسط یک برهان با کوچک‌ترین عدد گودل قابل اثبات بود. بنابراین پیچیدگی p بیشترین رمز Φ_e می‌باشد. امّا در رمزنگاری تعیین شده با π^n آن 0 است ($\pi^e(e) = 0$) و لذا $K^e(p) = 0$. از طرف دیگر اثبات $K^e(p) > 0$ را داشتیم. با فرض صحّت، این درست است. که تناقض می‌باشد. $\square$

قضیه ۳۶.۰.۴. *برای هر نظریه صوری $\mathbf{T}$ که توسیع PA باشد، ثابت مشخصه شایتین، $c_{\mathbf{T}}$، می‌تواند به طور دلخواه بزرگ باشد.*

برهان. فرض کنید که Φ ماشین تورینگی باشد که اصول $\mathbf{T}$ را چاپ کرده و متوقف می‌شود. به سادگی فرض می‌کنیم که رمز این ماشین 1 باشد. و فرض کنید که $\mathbf{T}$ به قدر کافی قوی است که ثابت کند Φ اصولش را چاپ کرده و متوقف می‌شود.

حالت اولیّه با I_Φ نشان داده شده است. ماشین تورینگ بعدی را به صورت $q_1 00 q_1$ در نظر بگیرید. واضح است که این ماشین تورینگ حتی شروع به کار نمی‌کند و این حقیقت بدیهی حتماً در هر نظریه صوری شامل حساب ابتدایی قابل اثبات است. حال یک رمزنگاری را به طریق زیر تعیین کنید: رمز ماشین تورینگ بالا را 2 در نظر بگیرید و مقدار n را بالا ببرید (به طور مثال $n = 10^{10^{10^{10}}}$). به ازای هر $k \leq n$، ماشین تورینگ Φ_k را شامل دستور $q_1 00 q_1$ که $k-1$ بار تکرار شده در نظر بگیرید. بدیهی است که می‌توان در $\mathbf{T}$ ثابت کرد که هیچ یک از این ماشین‌ها چیزی چاپ نمی‌کنند (حتی شروع به کار هم نمی‌کنند). حال ماشین تورینگ Φ_{n+1} را شامل دستور $I_\Phi 01 q_1$ در نظر بگیرید و این یعنی اینکه ماشین عدد 1 را چاپ کرده و متوقف می‌شود. عملکرد این ماشین همواره در PA قابل اثبات است. بنابراین، ما می‌توانیم $K(1) > n$ را در $\mathbf{T}$ ثابت کنیم. لذا طبق تعریف ۳۴.۰.۴، ثابت مشخصه‌ی نظریه $\mathbf{T}$، $c^{\Phi}_{\mathbf{T}}$، می‌بایست حتی بزرگ‌تر از این باشد. و البته، عدد n می‌تواند بزرگ‌تر از خواسته ما انتخاب شود. □

نتیجه ۳۷.۰.۴. *با توجه به روند اثبات قضیه فوق، پیچیدگی اصول $\mathbf{T}$ تحت این رمزنگاری 1 است. لذا تحت این رمزنگاری، $\mathbf{T}$ می‌تواند یک رشته (عدد) خاص را اثبات کند که پیچیدگی بیشتری از اصول خودش دارد. پس به این ترتیب، تعبیر عمومی از نتیجه شایتین، که $c^{\Phi}_{\mathbf{T}}$ محتوای اطلاعاتی یا میزان قدرت نظریه صوری $\mathbf{T}$ را اندازه‌گیری می‌کند و $\mathbf{T}$ نمی‌تواند ثابت کند هیچ شیئی با پیچیدگی کولموگروف بیشتر از $c^{\Phi}_{\mathbf{T}}$ وجود دارد، رد می‌شود.*

گزاره ۳۸.۰.۴. *برای هر نظریه‌ی $\mathbf{T}$ و ماشین تورینگ جهانی Φ داریم $r^{\Phi}_{\mathbf{T}} \leq c^{\Phi}_{\mathbf{T}}$.*

برهان. n را طوری در نظر بگیرید که با خروجی‌های $\{\Phi_0, \Phi_1, ..., \Phi_{r_{\mathbf{T}}-1}\}$ برابر نباشد. $\mathbf{T}$ ثابت می‌کند که هیچ یک از ماشین‌های تورینگ Φ_i برای $i < r_{\mathbf{T}}$، n را تولید نمی‌کند. چون اگر Φ_i جمله‌ای

را که ادعا می‌کند Φ_i خروجی m را می‌دهد، متوقف کند، توسط یک Σ_1ـ جمله بیان شده است، بنابراین $\Phi_i \not\downarrow n$ در $\mathbf{T}$ قابل اثبات است؛ و اگر Φ_i متوقف نکند، با کمینگی $r_{\mathbf{T}}$، $\Phi_i \not\downarrow n$ هم قابل اثبات است. $\mathbf{T}$ ثابت می‌کند که $r_{\mathbf{T}} - 1 < K(n)$ است، بنابراین $r_{\mathbf{T}} - 1 < c_{\mathbf{T}}$ می‌باشد. □

توجه داشته باشید که اگر Φ_i، $A_{\mathbf{S},\mathbf{T}}$ باشد آنگاه $i \leq c_{\mathbf{T}}$ و $c_{\mathbf{S}}$ خواهد بود، بنابراین با قرار دادن $\Phi_0 = A_{\mathbf{S},\mathbf{T}}$، می‌توانیم $r_{\mathbf{T}} = r_{\mathbf{S}} = c_{\mathbf{T}} = c_{\mathbf{S}}$ بسازیم.

لم ۳۹.۰.۴. *دو نظریه $\mathbf{S}$ و $\mathbf{T}$ را در نظر بگیرید که توسیع PA هستند و Φ یک ماشین تورینگ جهانی است. Π_1ـ جمله‌ی τ را در نظر بگیرید که در $\mathbf{T}$ قابل اثبات است ولی در $\mathbf{S}$ نیست. در این صورت:*

۱. *اگر Φ_0 یکی از D^0_τ یا $D^{(0)}_\tau$ باشد، آنگاه خواهیم داشت $r_{\mathbf{S}} < r_{\mathbf{T}}$.*

۲. *اگر $\{\Phi_0, \Phi_1\} = \{A^{(0)}_{\mathbf{S},\mathbf{T}}, D^0_\tau\}$ باشد، آنگاه خواهیم داشت $c_{\mathbf{S}} < c_{\mathbf{T}}$.*

برهان. ۱. با توجه به بند اوّل لم ۳۰.۰.۴ و لم ۳۱.۰.۴، PA، $\tau \longleftrightarrow\uparrow D_\tau \longleftrightarrow\uparrow D^{(0)} \longleftrightarrow\uparrow D^0_\tau$ را اثبات می‌کند. بنابراین Φ_0 یک ماشین تورینگ با کم‌ترین اندیسی است که متوقف نمی‌شود و عدم توقف آن توسط $\mathbf{S}$ قابل اثبات نیست. بنابراین $r_{\mathbf{S}} = 0$ و $r_{\mathbf{T}} > 0$.

۲. ماشین تورینگ جهانی Φ را طوری در نظر بگیرید که $\{\Phi_0, \Phi_1\} = \{A^{(0)}_{\mathbf{S},\mathbf{T}}, D^0_\tau\}$ باشد. با برهان زیر در $\mathbf{T}$ خواهیم داشت $c_{\mathbf{T}} > 1$. با τ، D_τ متوقف نمی‌شود. بنابراین D^0_τ هیچ کدام نمی‌باشد. برای هر n، $D^0_\tau \not\downarrow n$. و لذا 0 توسط $A^{(0)}_{S,\mathbf{T}}$ و D^0_τ تولید نشده است. از این رو $1 < K(0)$. حال ثابت می‌کنیم که $c_{\mathbf{S}} \leq 1$ است. اگر چنین نباشد، nای خواهیم داشت که $\mathbf{S}$ هیچ یک از $A^{(0)}_{\mathbf{S},\mathbf{T}}$ و D^0_τ را که n را تولید می‌کنند، اثبات نمی‌کند. اگر $n \neq 0$ باشد، با توجه به بند چهارم لم ۳۰.۰.۴، $\mathbf{S}$، $A_{\mathbf{S},\mathbf{T}} \not\downarrow n$ را اثبات می‌کند در حالی که متناقض با روند ساخت $A_{\mathbf{S},\mathbf{T}}$ می‌باشد. فرض کنید که $n = 0$ باشد. با توجه به بند دو لم ۳۰.۰.۴، $D^0_\tau \not\downarrow n$ ایجاب می‌کند که $D^0_\tau \uparrow$. بنابراین $D_\tau \uparrow$ و τ را داریم. امّا با توجه به فرضمان $\mathbf{S}$ نمی‌تواند τ را اثبات کند و داریم $c_{\mathbf{S}} < c_{\mathbf{T}}$. □

لم ۴۰.۰.۴. *فرض کنید $\psi(x)$ یک Δ_0ـ فرمول در $\mathcal{L}_A$ باشد. آنگاه کد m_0ای از یک ماشین تورینگ موجود است به طوری که*

$\mathtt{PA} \vdash \psi(x) \longleftrightarrow \Phi_{m_0}(x) \downarrow 1$ و

$\mathtt{PA} \vdash \neg\psi(x) \longleftrightarrow \Phi_{m_0}(x) \downarrow 0$.

برهان. $\psi(x)$ را یک Δ_0ـ فرمول دلخواه و ماشین تورینگ Φ_{m_0} را که در ادامه تعریف می‌شود در نظر بگیرید: Φ_{m_0} برهانی برای $\psi(x)$ یا $\neg\psi(x)$ از PA را جستجو کرده و اگر برهانی برای $\psi(x)$ یافت متوقف شده و خروجی 1 را بدهد و اگر برهانی برای $\neg\psi(x)$ یافت متوقف شده و خروجی 0 را بدهد. فرض کنید که $\mathtt{PA} \vdash \psi(\mathtt{x})$، در اینصورت با توجّه به روند ساخت Φ_{m_0}، $\Phi_{m_0} \downarrow 1$؛ و اگر $\mathtt{PA} \vdash \neg\psi(\mathtt{x})$ آنگاه $\Phi_{m_0} \downarrow 0$. برای عکس، اگر $\Phi_{m_0} \downarrow 1$ در اینصورت با توجّه به توضیحات فوق، Φ_{m_0} برهانی برای $\psi(x)$ را از PA یافته است؛ پس $\mathtt{PA} \vdash \psi(\mathtt{x})$. و اگر $\Phi_{m_0} \downarrow 0$، Φ_{m_0} برهانی برای $\neg\psi(x)$ را از PA یافته است؛ پس $\mathtt{PA} \vdash \neg\psi(\mathtt{x})$. □

لم ۴۱.۰.۴. *فرض کنید $\psi(x)$ یک Δ_0ـ فرمول در $\mathcal{L}_A$ باشد. آنگاه کدی مانند m از یک ماشین تورینگ موجود است به طوری که*

$$\mathtt{PA} \vdash \forall x \psi(x) \longleftrightarrow \Phi_m \uparrow .$$

برهان. فرض کنید Φ_{m_0} ماشین تورینگی باشد که با توجه به لم ۴۰.۰.۴ می‌توانیم برای $\psi(x)$ در نظر بگیریم. فرض کنید Φ_m یک ماشین تورینگ متناظر با برنامه C که در زیر بیان شده است باشد:

$$\text{while} \quad (\psi(x))$$
$$Do \quad x := x + 1$$

Φ_m را دقیق‌تر توضیح می‌دهیم. I_M حالت اولیه Φ_m است. Φ_m مقدار x را ذخیره می‌کند که می‌توانیم بعداً بازیابی کنیم. پس Φ_m، $\psi(x)$ را با نقش Φ_{m_0} ارزیابی می‌کند. اگر مقدار 0 باشد، پس به حالت نهایی و یکتای q_f وارد شده و متوقف می‌شود. اگر مقدار 1 باشد پس مقدار x به قطعه اولیه نوار بازیابی می‌شود. پس Φ_m مقدار x را توسط 1 افزایش می‌دهد و حالت اولیه را I_M وارد می‌کند.

حال، لم را نشان می‌دهیم. ما در PA کار می‌کنیم. فرض کنید $\forall x \psi(x)$ را داشته باشیم. می‌توانیم فرمولی در $\mathcal{L}_A$ نشان دهیم که بر ادعای زیر دلالت دارد:

ادعا ۴۲.۰.۴. برای تمام n ها، پردازشی از Φ_m با ورودی 0 موجود است که ID نهایی دارای حالت اولیه بوده و محتوای نوار n است.

این واضح است که پردازش با ID منحصر به فرد $\langle I_M, bin(0), 0\rangle$ پردازشی برای $n=0$ است. فرض کنید $n \geq 1$ باشد. با فرض استقراء، پردازشی از Φ_m با ورودی 0 موجود است که ID نهایی آن $\langle I_M, bin(n-1), 0\rangle$ است. چون $\forall x\psi(x)$، پردازش‌های p_n را برای $\Phi_{m_0} \downarrow 1$ داریم. می‌توانیم پردازش‌های p_n را الحاق کرده و پردازشی برای اجرای $x++$ که قبلاً به‌دست آمده داشته باشیم. پردازشی با ID نهایی $\langle I_M, bin(n), 0\rangle$ را داریم. بنابراین، ادعا برقرار است و در نتیجه داریم $\Phi_m \uparrow$.
برای عکس، فرض کنید که $\Phi_m \uparrow$ را داشته باشیم. می‌توانیم فرمولی در $\mathcal{L}_A$ بیان کنیم که بر ادعای زیر دلالت دارد:

ادعا ۴۳.۰.۴. برای تمام nها، پردازش Φ_m با ورودی 0 موجود است به طوری که ID نهایی $\langle I_M, bin(n), 0\rangle$ است و اگر n 0 باشد آنگاه داریم $\psi(n-1)$.

این ادعا را با استقرا روی n اثبات می‌کنیم. برای $n=0$ واضح است. فرض کنید $n \geq 1$ باشد. با فرض استقراء، پردازش Φ_m با ورودی 0 موجود است به طوری که ID نهایی $\langle I_M, bin(n-1), 0\rangle$ است. با توجه به لم ۴۰.۰.۴، برای $\Phi_{m_0}(n-1) \downarrow 0$ یا $\Phi_{m_0}(n-1) \downarrow 1$ پردازشی وجود دارد. در حالتی که $\Phi_{m_0}(n-1) \downarrow 0$، کنترل q_f را وارد کرده و داریم $\Phi_m \downarrow$. این متناقض با فرضمان می‌باشد. بنابراین، پردازشی برای $\Phi_{m_0}(n-1) \downarrow 1$ موجود است. درنتیجه، باتوجه به لم ۴۰.۰.۴ داریم $\psi(n-1)$. حال، می‌توانیم نوار ارزش x را از $n-1$ به n افزایش دهیم. بنابراین ادعا درست است. لذا با توجه به ادعا، داریم $\forall x\psi(x)$. $\square$

قضیه ۴۴.۰.۴. *فرض کنید که $\mathbf{T}$ و $\mathbf{S}$، نظریه‌های صوری صحیح، به طور بازگشتی اصل‌پذیر و توسیع* PA *باشند به طوری که $\mathbf{T} < \mathbf{S}$ باشد. گزاره‌های زیر معادلند:*

۱. *Π_1ـ جمله‌ی θ موجود است به طوری که داریم $\mathbf{T} \vdash \theta$ اما $\mathbf{S} \nvdash \theta$.*

۲. *شمارشی از ماشین‌های تورینگ موجود است به طوری که داریم $r_{\mathbf{T}} < r_{\mathbf{S}}$.*

برهان. فرض کنید که (۱) برقرار باشد و θ را Π_1ــ جمله‌ای در نظر بگیرید که (۱) را ارضا می‌کند. از آنجایی که $\mathbf{T} \vdash \theta$ و $\mathbf{S} \nvdash \theta$، با استفاده از لم ۴۱.۰.۴ می‌توان نتیجه گرفت که کدی مانند m از یک ماشین تورینگ وجود دارد که $\mathbf{T} \vdash \Phi_m \uparrow$ و $\mathbf{S} \nvdash \Phi_m \uparrow$. بنابراین، با توجّه به تعریف ثابت مشخصه راتیکاینن، $m < r_{\mathbf{T}}$ و $r_{\mathbf{S}} \leq m$ لذا $r_{\mathbf{S}} < r_{\mathbf{T}}$. برای عکس، فرض کنید که $r_{\mathbf{S}} < r_{\mathbf{T}}$ باشد. در اینصورت $\mathbf{T}$، Π_1ــ جمله‌ی $\Phi_{r_{\mathbf{S}}} \uparrow$ را اثبات می‌کند در حالی که $\mathbf{S}$ نمی‌تواند آن را اثبات کند. $\square$

در قضیه ۴۴.۰.۴ ثابت کردیم که برای برخی از ماشین‌های تورینگ جهانی $r_{\mathbf{S}} < r_{\mathbf{T}}$ اگر و فقط اگر Π_1ــ جمله‌ی قابل اثبات در $\mathbf{T}$ موجود باشد که در $\mathbf{S}$ قابل اثبات نیست که این نیز به عنوان نتیجه‌ای از قضیه زیر به دست می‌آید.

قضیه ۴۵.۰.۴. *دو نظریه* $\mathbf{S}$ *و* $\mathbf{T}$ *را در نظر بگیرید که توسیع* PA *هستند. گزاره‌های زیر معادلند:*

۱ . *Π_1ــ جمله‌ای مانند τ موجود است که در $\mathbf{T}$ قابل اثبات است ولی در $\mathbf{S}$ نیست.*

۲ . *برای برخی از ماشین‌های تورینگ جهانی، $r_{\mathbf{S}} = r_{\mathbf{T}}$ و $c_{\mathbf{S}} < c_{\mathbf{T}}$ می‌باشد.*

۳ . *برای برخی از ماشین‌های تورینگ جهانی، $r_{\mathbf{S}} < r_{\mathbf{T}}$ و $c_{\mathbf{S}} < c_{\mathbf{T}}$ می‌باشد.*

۴ . *برای برخی از ماشین‌های تورینگ جهانی، $r_{\mathbf{S}} < r_{\mathbf{T}}$ و $c_{\mathbf{S}} = c_{\mathbf{T}}$ می‌باشد.*

برهان. فرض کنید که (۱) برقرار باشد. ماشین تورینگ جهانی Φ را طوری در نظر بگیرید که $(\Phi_0, \Phi_1) = (A^{(0)}_{\mathbf{S},\mathbf{T}}, D^0_\tau)$ باشد. با توجه به بند دو لم ۳۹.۰.۴، $c_{\mathbf{S}} < c_{\mathbf{T}}$ را داریم. از طرفی چون هیچ کدام از $\mathbf{S}$ و $\mathbf{T}$، $A^{(0)}_{\mathbf{S},\mathbf{T}} \uparrow$ را اثبات نمی‌کند لذا بند اوّل لم ۳۰.۰.۴، $r_{\mathbf{S}} = r_{\mathbf{T}} = 0$ را در پی دارد. در نتیجه (۲) درست است. با در نظر گرفتن (۲) و بند اوّل لم ۳۹.۰.۴ و این که $(\Phi_0, \Phi_1) = (D^0_\tau, A^{(0)}_{\mathbf{S},\mathbf{T}})$ است (۳) را خواهیم داشت. برای (۴)، قرار می‌دهیم $(\Phi_0, \Phi_1) = (D^{(0)}_\tau, A_{\mathbf{S},\mathbf{T}})$. چون ثابت مشخصه با عملگر $^{(0)}$ ترقی یافته و توسط $A_{\mathbf{S},\mathbf{T}}$ محدود شده، پس داریم $c_{\mathbf{S}} = c_{\mathbf{T}} = 1$. برای عکس، اگر $c_{\mathbf{S}} < c_{\mathbf{T}}$ باشد، عدد طبیعی nای موجود است به طوری که $\mathbf{T}$، $\Phi_0 \not\downarrow n \wedge \Phi_1 \not\downarrow n \wedge \ldots \wedge \Phi_{c_{\mathbf{T}}} \not\downarrow n$ را ثابت می‌کند. برای برخی از iها که $i < c_{\mathbf{T}}$ است، $\mathbf{S}$، $\Phi_i \not\downarrow n$ را ثابت نمی‌کند که یک Π_1جمله است. اگر $r_{\mathbf{S}} < r_{\mathbf{T}}$ باشد آنگاه $\mathbf{T}$، Π_1ــ جمله‌ی $\Phi_{r_{\mathbf{S}}} \uparrow$ را اثبات می‌کند در حالی که $\mathbf{S}$ نمی‌تواند آن را اثبات کند. $\square$

تذکر ۴.۰.۴۶. ما نیازی نداریم که فرض کنیم $\mathbf{T}$ نظریه‌ی قوی‌تری از $\mathbf{S}$ است تا ثابت کنیم $c_{\mathbf{S}} < c_{\mathbf{T}}$ یا $r_{\mathbf{S}} < r_{\mathbf{T}}$. از طرف دیگر، اختلاف بین $c_{\mathbf{T}}$ و $r_{\mathbf{T}}$ نسبت به یک ماشین تورینگ جهانی کران‌دار نیست.

گزاره ۴.۰.۴۷. *برای هر ماشین تورینگ جهانی بدون ورودی Φ و هر عدد طبیعی دلخواه n، ماشین تورینگ جهانی Ψ موجود است به طوری که $K^{\Phi} = K^{\Psi}$، $r_{\mathbf{T}}^{\Phi} = r_{\mathbf{T}}^{\Psi}$ و $c_{\mathbf{T}}^{\Psi} < r_{\mathbf{T}}^{\Psi} + n$.*

برهان. برای هر $l \leq r_{\mathbf{T}}^{\Phi} + n + 1$، یک ماشین تورینگ جهانی تعریف می‌کنیم به طوری که برای هیچ $i \leq r_{\mathbf{T}}^{\Phi} + n$، j ای موجود نباشد که $\Psi_{li} = \Psi_{lj}^{(l)}$ برقرار شود. $\mathbf{T}$ ثابت می‌کند که l نمی‌تواند توسط هیچ یک از Ψ_{l_0} و Ψ_{l_1} و ... و $\Psi_{lr_{\mathbf{T}}^{\Phi}+n}$ تولید شده باشد و در نتیجه داریم $r_{\mathbf{T}}^{\Phi} + n < K^{\psi_l}(l)$. از طرف دیگر، چون $\mathbf{T}$ برای تمام $i \leq r_{\mathbf{T}}^{\Phi} + n$، $\Phi_i \uparrow \longleftrightarrow \Psi_{li} \uparrow$ را ثابت می‌کند، داریم $r_{\mathbf{T}}^{\Phi} = r_{\mathbf{T}}^{\Psi_l}$. حداقل یکی از این l ها همواره $K^{\Phi} = K^{\Psi_l}$ را ارضا می‌کند. N را مجموعه‌ی خروجی‌های Ψ_{l_0} و Ψ_{l_1} و ... و $\Psi_{lr_{\mathbf{T}}^{\Phi}+n}$ در نظر بگیرید. چون N شامل حداکثر $r_{\mathbf{T}}^{\Phi} + n + 1$ عضو است، می‌توانیم $l_0 \leq r_{\mathbf{T}}^{\Phi} + n + 1$ در نظر بگیریم که در N ظاهر نمی‌شود. پس داریم $r_{\mathbf{T}}^{\Phi} + n < K^{\Phi}(l_0)$ و در نتیجه $K^{\Phi} = K^{\Psi_{l_0}}$ برقرار است. □

مراجع

[1] Z. Adamowicz and P. Zbierski, *Logic of Mathematics: a modern course of classical logic,* (Wiley, 1997).

[2] J. Barwise, *Comments Introducing Boolos' Article,* Notices Am. Math. Soc. (1989).

[3] G. Boolos, *A New Proof of the Gödel Incompleteness Theorem,* Notices Am. Math. Soc. 36(4) 388–290 (1989).

[4] G. Boolos, The Logic of Provability, Cambridge University Press (Cambridge 1997).

[5] G. Chaitin, *Information-Theoretic Limitations of Formal Systems,* IEEE Trans. Inf. Theory 21(3) 403–424 (1974).

[6] K. Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I,* Monatsh. Math. Phys. 38(1) 173–198 (1931).

[7] S. Ibuka, M. Kikuchi and H. Kikyo, *Kolmogorov Complexity and Characteristic Constants of Formal Theories of Arithmetic*, Math. Log. Quart. 57(5), 470–473 (2011).

[8] R. Kaye, *Models of Peano Arithmetic* (Oxford University Press, 1991).

[9] R. Kaye and H. Kotlarski, *On Models Constructed by Means of the Arithmetized Completeness Theorem,* Math. Log. Q. 46(4) 505–516 (2000).

[10] M. Kikuchi, *A Note on Boolos' Proof of the Incompleteness Theorem,* Math. Log. Q. 40(4) 528–532 (1994).

[11] M. Kikuchi, *Kolmogorov Complexity and the Second Incompleteness Theorem,* Arch. Math. Log. 36(6) 437–443 (1997).

[12] M. Kikuchi and K. Tanaka, *On Formalization of Model-Theoretic Proofs of Gödel's Theorems,* Notre Dame J. Formal Log. 35(3) 403–412 (1994).

[13] M. Kikuchi, T. Kurahashi, and H. Sakai, *On Proofs of The Incompleteness Theorems Based on Berry's paradox By Vopěnka, Chaitin, and Boolos,* Math. Log. Quart. 58(4–5) 307–316 (2012).

[14] H. Kotlarski, *On the Incompleteness Theorems,* J. Symb. Log. 59(4) 1414–1419 (1994).

[15] H. Kotlarski, *The Incompleteness Theorems After 70 Years,* Ann. Pure Appl. Log. 126(1–3) 125–138 (2004).

[16] G. Kreisel, *A Survey of Proof Theory,* J. Symb. Log. 33(3) 321–388 (1968).

[17] S. Maehara, *Boolos shi no genkou wo mite,* Gendai Shisou (December issue) 80–92 (1989); in Japanese.

[18] P. Raatikainen, *On Interpreting Chaitin's Incompleteness Theorem*, Journal of Philosophical Logic 27(6) 569–586 (1998).

[19] B. Russell, *Mathematical Logic is Based on the Theory of Types,* Am. J. Math. 30(3) 222–262 (1908).

[20] C. Smoryński, *The Incompleteness Theorems,* in Handbook of Mathematical Logic, edited by J. Barwise (North-Holland 1977) pp. 821–865.

[۲۱] ف. آذرپیوند، *خودنامصداقی و ناتمامیت*، پایان‌نامه کارشناسی ارشد، دانشکده ریاضی، دانشگاه تبریز، ۱۳۹۰.

[۲۲] ح. شیرزاده، *کوتاهترین تعریف یک عدد در حساب پئانو*، پایان‌نامه کارشناسی ارشد، دانشکده ریاضی، دانشگاه تبریز، ۱۳۹۲.

[۲۳] پ. قائمی، *پارادوکس آزمون ناگهانی و قضیه دوم ناتمامیت*، پایان‌نامه کارشناسی ارشد، دانشکده ریاضی، دانشگاه تبریز، ۱۳۹۲.

واژه‌نامه فارسی به انگلیسی

اثبات‌پذیری	Provability
استدلال	Argument
استقراء	Induction
استنتاج	Deduction
اصل	Principle
اصل موضوع	Axiom
بازگشتی	Recursive
برهان	Proof
پارادوکس	Paradox
پارادوکس بِری	Berry’s Paradox
پیچیدگی	Complexity
پیچیدگی کولموگروف	Kolmogrov complexity
تصمیم‌ناپذیری	Undecidablitity
تناقض	Contradiction
ثابت	Constant
جایگزینی	Substitution
جمله مستقل	Independent Sentence
حساب	Arithmetic

حکم .... Statement
زبان .... Language
سازگار .... Consistent
سور .... Quntifier
شرایط .... Condition
شمارش‌پذیر .... Enumerable
صحیح .... Sound
صدق‌پذیری .... Satisfiable
صوری .... Formal
عددگودل .... number Gödel
عکس نقیض .... Contraposition
عملگر .... Operator
فرمول .... Formula
قابل توصیف .... Describable
قضایای ناتمامیت گودل .... Gödel’s Incompleteness Theorems
قضیه .... Theorem
قطری‌سازی .... Diagonalization
کدگذاری .... Encoding
ماشین تورینگ .... Turing Machine
متغیر .... Variable
متغیر آزاد .... Variable Free
متناهی .... Finite
محاسبه‌پذیر .... Computable
محمول .... Predicate
معادله .... Equation

معنایی .... Semantic
منطق گزاره‌ای .... Logic Propositional
ناسازگار .... Inconsistent
نتیجه .... Conclusion
نظریه .... Theory
نقیض .... Negation
نمایش‌پذیری .... Representable
وضع مقدم .... Ponens Modus
هم‌ارز .... Equivalent

واژه‌نامه انگلیسی به فارسی

Argument	استدلال، شناسه
Arithmetic	حساب
Arithmetization	حسابی کردن
Arithmetized	حسابی
Axiom	اصل
Axiomatizable	اصل‌پذیر
Axiom schema	شمای اصل موضوعی
Berry’s paradox	پارادوکس بری
Complete	تمام
Complexity	پیچیدگی
Computable	محاسبه‌پذیر
Consistent	سازگار
Contradiction	تناقض
Corollary	نتیجه
Definable	تعریف‌پذیر
Derivability	اثبات‌پذیری
Derivable	اثبات‌پذیر
Derived	اثبات‌شده

Diagonalization .... قطری‌سازی
Encoding .... کدگذاری
Factorization .... فاکتورگیری
Formal .... صوری
Formula .... فرمول
Formalized .... صوری سازی
Generalization .... عمومی
Incompleteness .... ناتمامیت
Inconsistent .... ناسازگار
Isomorphic .... ایزومورف
Kolomogorov Complexity .... پیچیدگی کولوموگروف
Named .... توصیف
Non-logical .... غیر منطقی
Partial .... جزئی
Pigeonhole Principle .... اصل لانه کبوتر
Primitive .... ابتدایی
Provable .... اثبات‌پذیر
Provability .... اثبات‌پذیر
Recursive .... بازگشتی
Recursively Axiomatizable .... بازگشتی اصل‌پذیر
Representable .... نمایش‌پذیر
Representing .... به نمایندگی
Satisfies .... ارضا
Satisfying .... ارضاپذیری
Sound .... درست

کلی .... Total

ماشین تورینگ .... Turing Machine

متغیر .... Variable

متغیر آزاد .... Free Variable

Surname: Sarvari Mehrabad **Name:** Sonia

Title: On Proofs of the Incompleteness Theorems Based on Berry's Paradox

Supervisor: Saeed Salehi

Advisor: Hazhir Homei

Degree: Master of Science **Subject:** Pure Mathematics

Field: Mathematical Logic **University of Tabriz**

Faculty of Mathematical Sciences **Date:** 2015 **Number of Pages:** 46

Keywords: The Incompleteness Theorems, Berry's Paradox, Kolmogorov Complexity.

Abstract

By formalizing Berry's paradox, Vopěnka, Chaitin, Boolos and others proved the incompleteness theorems without using the diagonal argument. In this Thesis, we examine these proofs closely and show their relationships. Firstly, we show that one can use the diagonal argument for proofs of the incompleteness theorems based on Berry's paradox. Then, we show that an extension of Boolos' proof can be considered as a special case of Chaitin's proof by defining a suitable Kolmogorov complexity.

University of Tabriz

Faculty of Mathematical Sciences

DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN PURE MATHEMATICS

On Proofs of the Incompleteness Theorems Based on Berry's Paradox

Supervisor

Saeed Salehi

Advisor

Hazhir Homei

By

Sonia Sarvari Mehrabad

2015