دانشگاه تبریز

دانشکده علـوم ریاضی

گروه ریاضی محض

پایان‌نامه

برای دریافت درجه کارشناسی ارشد در رشته‌ی

ریاضی محض، گرایش منطق

عنوان

پیچیدگی کولموگروف و ثوابت مشخصه‌ی نظریه‌های صوری حساب

استاد راهنما

دکتر سعید صالحی پورمهر

استاد مشاور

دکتر هژیر حومئی

پژوهشگر

سجّاد غنی‌زاده زارع

۱۳۹۴

ستایش

ستایش می کنم کسی را که منّتش عظیم است و نعمتش فراوان؛ و رحمتش بر غضبش پیشی گرفته است. سخن و حکم او تمامیّت یافته و قطعی است؛ خواست او نافذ و برهانش رسا و حکمش بر عدالت است.

ستایش می کنم به سان سپاس آن که معترف به ربوبیّتش و پر خضوع در بندگی اوست. و از گناه خویش (بریده) کنده شده و به توحید او اقرار می نماید. و از وعید و بیم عذابش به خود او پناه می برد. و از درگاه پروردگارش امیدوار آمرزشی است که او را نجات بخشد، در روزی که (انسان را به گرفتاری خویش مشغول و) از بستگان و فرزندانش غافل می سازد.

از او یاری و هدایت می جوییم و به او ایمان داریم و بر او توکّل می کنیم. از ضمیری با اخلاص و یقین، برای او) به توحید) گواهی می دهم و او را به یکتایی می شناسم. یکتاشناسی فردی مؤمن و استوار (در یقین). و او را یگانه می شمارم، یگانه دانستن بنده ای خاضع. نه در پادشاهی خود شریکی دارد و نه در آفرینشش یاوری. برتر از آن است که مشاور و وزیری داشته باشد و منزّه است از داشتن همانند و نظیری بر کردارها آگاهی یافت و پوشیده داشت و از نهان امور مطّلع گردید و بدان آگاه است و اقتدار و چیرگی دارد. نافرمانی گشت و آمرزید، طاعت و بندگی اش نمودند و او شکرگزاری نمود.

فرمان روایی کرد و عدالت گسترد؛ و برتر از شائبه ی هر نقص و عیبی است و (آنچه شایسته ی هر چیزی بود، به او) عطا فرمود. همیشه بوده و هست و هیچ گاه زوال نمی یابد و چیزی همانندش نیست. و او پیش از هر چیزی است و پس از هر چیزی. پروردگاری است که به عزّتش یگانه و به قدرت خویش پادشاه (و مقتدر). و به برتری شأنش پاک (و منزّه) است. و به علوّ مقامش (به حق) خود را بزرگ می شمارد. دیده ای او را نمی بیند و نگرشی (در معرفت) بر او احاطه پیدا نمی کند. قوی و مقتدر و بینا و شنوا و برتر و حکیم و رئوف و مهربان و عزّتمند و داناست. هر آن که به توصیف او برآید، در وصفش حیران ماند. (به آفریدگان) نزدیک است و (در رفعت مقام، از آنان) دور است. .

خطبه بدون نقطه حضرت علی (ع) در مدح و ستایش خداوند

تقدیم به:

زیباترین مخلوقات هستی،

پدر بزرگوار، مادر عزیز

و

همسر گلم.

نام خانوادگی دانشجو: غنی‌زاده زارع نام: سجّاد

عنوان: پیچیدگی کولموگروف و ثوابت مشخصه‌ی نظریه‌های صوری حساب

استاد راهنما : دکتر سعید صالحی پورمهر

استاد مشاور : دکتر هژیر حومئی

مقطع تحصیلی: کارشناسی ارشد رشته: ریاضی محض گرایش: منطق دانشگاه تبریز

دانشکده علوم ریاضی تاریخ فارغ التحصیلی: ۱۳۹۴ تعداد صفحات: ۹۶

کلید واژه‌ها: پیچیدگی کولموگروف، ثابت مشخصه.

چکیده

این پایان‌نامه، به بحث در مورد دو ثابت مشخصه $c_{\mathbf{T}}$ و $r_{\mathbf{T}}$ که به ترتیب توسط شایتین و راتیکاینن برای هر نظریه به طور بازگشتی اصل‌پذیر و سازگار $\mathbf{T}$ که با استفاده از یک ماشین تورینگ جهانی تعریف شده می‌پردازد. راتیکاینن استدلال کرد که $c_{\mathbf{T}}$ پیچیدگی کولموگروف $\mathbf{T}$ را نشان نمی‌دهد و پی برد که برای دو نظریه $\mathbf{S}$ و $\mathbf{T}$، همواره می‌توان ماشین تورینگ جهانی یافت که $c_{\mathbf{T}} = c_{\mathbf{S}}$. در این پایان‌نامه که بر اساس مقاله های [۱۶]، [۱۷]، [۲۵] و [۳۳] نگاشته شده است نشان داده می‌شود که سه شرط زیر معادلند:

۱. Π_1–جمله‌ای مانند τ موجود است که در $\mathbf{T}$ قابل اثبات است ولی در $\mathbf{S}$ نیست.

۲. برای برخی از ماشین‌های تورینگ جهانی، $c_{\mathbf{S}} \neq c_{\mathbf{T}}$ برقرار است.

۳. برای برخی از ماشین‌های تورینگ جهانی، $r_{\mathbf{S}} \neq r_{\mathbf{T}}$ برقرار است.

همچنین نشان داده می‌شود که $r_{\mathbf{T}}$ لزوماً بر $c_{\mathbf{T}}$ منطبق نیست؛ و برای دو نظریه‌ی حسابی $\mathbf{T}$ و $\mathbf{S}$ با Π_1–جمله‌ای که در $\mathbf{T}$ اثبات‌پذیر است اما در $\mathbf{S}$ نیست، همواره شمارشی از ماشین‌های تورینگ وجود دارد به طوری که $c_{\mathbf{T}} = c_{\mathbf{S}}$ و $r_{\mathbf{S}} < r_{\mathbf{T}}$.

فهرست مطالب

مقدمـه

پیچیدگی شهودی اشیاء متناهی به صورت «پیچیدگی کولموگروف[۱]» به معنی مفهوم سختی توصیف یک شیء توسط شمارشی بازگشتی از تمام ماشین‌های تورینگ (یا یک ماشین تورینگ جهانی ثابت) صوری‌سازی می‌شود. شایتین[۲][۴] ثابت کرد که برای یک نظریه صوری به طور بازگشتی اصل‌پذیر و سازگار $\mathbf{T}$، یک عدد طبیعی به نام $c_{\mathbf{T}}$ طوری وجود دارد که نظریه $\mathbf{T}$ نمی‌تواند ثابت کند که شیئی با پیچیدگی کولموگروف بیشتر از $c_{\mathbf{T}}$ وجود دارد؛ حتی اگر بی‌نهایت اشیاء با این خاصیت (با پیچیدگی کولموگروف بیشتر از $c_{\mathbf{T}}$) وجود داشته باشند. این نتیجه (به اشتباه) این گونه تفسیر شد که «نظریه $\mathbf{T}$ جملاتی که دارای پیچیدگی بیشتری نسبت به خود $\mathbf{T}$ هستند را نمی‌تواند ثابت کند».

عدد $c_{\mathbf{T}}$ توسط فان لامبالگن[۳][۲۵] ثابت مشخصه $\mathbf{T}$ نامیده شد، و همو بود که با نشان دادن وجود نظریه‌هایی با پیچیدگی مختلف که ثابت مشخصه‌ی آن‌ها همان c_T است، به نگرش c_T به عنوان پیچیدگی نظریه $\mathbf{T}$ انتقاد کرد. راتیکاینن[۴][۳۳] روی انتخاب ماشین تورینگ به عنوان عاملی که در مقدار $c_{\mathbf{T}}$ تأثیر می‌گذارد متمرکز شده بود و در حقیقت ثابت کرد که برای هر نظریه صوری به طور بازگشتی اصل‌پذیر و سازگار $\mathbf{T}$، ماشین تورینگ جهانی موجود است به طوری که $c_{\mathbf{T}}$ برابر صفر می‌شود؛ بنابراین همواره ممکن است برای دو نظریه‌ی $\mathbf{T}$ و $\mathbf{S}$، تساوی $c_{\mathbf{T}} = c_{\mathbf{S}}$ برقرار باشد.

در این پایان‌نامه توصیفی از وجود یک ماشین تورینگ جهانی بر اساس مقاله های [۱۶]، [۱۷]،

[۱] Kolmogorov complexity

[۲] Chaitin

[۳] van Lambalgen

[۴] Raatikainen

[۲۵] و [۳۳] ارایه می‌شود به طوری که $c_{\mathbf{T}} \neq c_{\mathbf{S}}$ برقرار باشد: ثابت خواهد شد که برای برخی از ماشین‌های تورینگ جهانی $c_{\mathbf{S}} < c_{\mathbf{T}}$ برقرار است اگر و فقط اگر $\mathbf{T}$ یک Π_1-جمله‌ی حسابی را ثابت کند که $\mathbf{S}$ نمی‌تواند آن را ثابت کند. ثابت دیگر $r_{\mathbf{T}}$ توسط راتیکاینن [۳۳] در ارتباط با $c_{\mathbf{T}}$ معرفی شده است. نشان داده می‌شود که تفاوت بین $c_{\mathbf{T}}$ و $r_{\mathbf{T}}$ می‌تواند به هر اندازه دلخواه بزرگ باشد. از طرف دیگر، برای برخی از ماشین‌های تورینگ جهانی $r_{\mathbf{S}} < r_{\mathbf{T}}$ برقرار است اگر و فقط اگر برای برخی از ماشین‌های تورینگ جهانی (احتمالاً متفاوت) $c_{\mathbf{S}} < c_{\mathbf{T}}$ برقرار باشد.

فصل‌های مختلف این پایان‌نامه به صورت زیر است:

در فصل اول، تعاریف و مفاهیم اولیه‌ی نظریه محاسبات مورد نیاز را ارایه می‌دهیم. در فصل دوم، بیان می‌کنیم که ریاضیات شایتین نتایج فلسفیش را تایید نمی‌کند و دو کاربرد از نظریه الگوریتمی اطلاعی را مورد مطالعه قرار می‌دهیم. در فصل سوم، تفسیر شایتین از نتیجه‌اش را زیر سوال برده و سعی می‌کنیم که ماهیت درستی از ثابت مشخصه را در مسایل مورد تجزیه و تحلیل قرار دهیم و ببینیم چه عاملی مردم را به چنین تفسیری سوق می‌دهد. در فصل چهارم، به ثوابت مشخصه توسط پیچیدگی کولموگروف پرداخته، مفهوم ماشین تورینگ را در **PA** فرمول‌بندی می‌کنیم و نشان می‌دهیم که برای هر نظریه صوری صحیح مانند $\mathbf{T}$ که توسیع **PA** باشد، ثوابت مشخصه‌ی شایتین و راتیکاینن موجودند و همچنین نشان داده می‌شود که $r_{\mathbf{T}}$ لزوماً بر $c_{\mathbf{T}}$ منطبق نیست؛ و برای دو نظریه‌ی حسابی $\mathbf{T}$ و $\mathbf{S}$ با Π_1-جمله‌ای که در $\mathbf{T}$ اثبات‌پذیر است اما در $\mathbf{S}$ نیست، همواره شمارشی از ماشین‌های تورینگ وجود دارد به طوری که $c_{\mathbf{T}} = c_{\mathbf{S}}$ و $r_{\mathbf{S}} < r_{\mathbf{T}}$. در فصل پنجم، به صورت مفصل به پیچیدگی کولموگروف و ثوابت مشخصه نظریه‌های صوری حساب پرداخته، نشان می‌دهیم که مقدار $c_{\mathbf{T}}$ علاوه بر قدرت نظریه صوری $\mathbf{T}$، به انتخاب ماشین تورینگ جهانی نیز بستگی دارد و با انتخاب ماشین تورینگ مناسب می‌توان مقدار $c_{\mathbf{T}}$ را صفر یا به طور دلخواه بزرگ کرد و در پایان نشان داده می‌شود که برای نظریه‌های صوری صحیح $\mathbf{T}$ و $\mathbf{S}$ که توسیع **PA** باشند سه شرط زیر معادلند:

۱. Π_1-جمله‌ای مانند τ موجود است که در $\mathbf{T}$ قابل اثبات است ولی در $\mathbf{S}$ نیست.

۲. برای برخی از ماشین‌های تورینگ جهانی، $c_{\mathbf{S}} \neq c_{\mathbf{T}}$ برقرار است.

۳. برای برخی از ماشین‌های تورینگ جهانی، $r_{\mathbf{S}} \neq r_{\mathbf{T}}$ برقرار است.

فصل ۱

تعاریف و مفاهیم اولیه

این فصل شامل تعریف‌های اساسی و پایه‌ای است که در فصل‌های بعد برای درک بیشتر به آن‌ها نیاز خواهیم داشت. از این رو تعریف یک نظریه[۱]، حساب پئانو[۲] و ماشین تورینگ[۳] که در فصل‌های بعد به کرات با آن‌ها روبرو خواهیم شد، در این فصل گنجانده شده است.

۱.۱ مبادی نظریه محاسبه

تعریف ۱.۱.۱. (الفبا [۲۷]). یک الفبا مجموعه‌ای متناهی مانند Σ است. هر دنباله‌ی متناهی از اعضای Σ را یک «کلمه» یا «رشته» می‌نامند. مجموعه‌ی همه‌ی دنباله‌های متناهی متشکل از اعضای مجموعه‌ی Σ را با Σ^* نشان می‌دهیم.

تعریف ۱.۱.۲. (الفبای زبان‌های مرتبه اول [۱۴]). الفبای یک زبان مرتبه اول $\mathcal{L}$، شامل موارد زیر است:

(۱) همه روابط گزاره‌ای اعم از $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$، نمادهای $\exists$ و $\forall$ (به ترتیب سور وجودی و سور عمومی)، یک مجموعه شمارای $x_1, x_2, \ldots$ (متغیرها) و پرانتزها (و).

(۲) به علاوه، الفبای $\mathcal{L}$ می‌تواند شامل موارد زیر باشد:

(الف) یک مجموعه متناهی یا شمارا از نمادهایی چون P که نماد محمولی نامیده می‌شوند.

(ب) یک مجموعه متناهی یا شمارا از نمادهایی چون c که نماد ثابت نامیده می‌شوند.

(پ) یک مجموعه متناهی یا شمارا از نمادهایی چون f که نماد تابعی نامیده می‌شوند.

تعریف ۱.۱.۳. (زبان صوری [۱۳]). هر زیرمجموعه $\mathcal{L}$ از Σ^* را یک زبان (صوری) با الفبای Σ، یا یک زبان روی (الفبای) Σ، می‌گوییم.

تعریف ۱.۱.۴. (زبان تصمیم‌پذیر [۱۳]). یک زبان $\mathcal{L}$ روی الفبای Σ را تصمیم‌پذیر گوییم، هرگاه

---

[۱] Theory

[۲] Peano Arithmetic

[۳] Turing machine

الگوریتمی[۱] وجود داشته باشد که به ازای هر ورودی $\sigma \in \Sigma^*$، تعیین کند که آیا $\sigma \in \mathcal{L}$ یا $\sigma \notin \mathcal{L}$ برقرار هستند.

تعریف ۵.۱.۱. (شمارای کارآمد [۱۳]). زبان $\mathcal{L}$ روی الفبای Σ را شمارای کارآمد گوییم هرگاه الگوریتمی بدون ورودی موجود باشد که خروجی‌های آن دقیقاً اعضای $\mathcal{L}$ باشند.

در تعریفی معادل برای مفهوم شمارای کارآمد می‌توان گفت که مجموعه‌ی $A \subseteq \Sigma^*$ شمارای کارآمد است اگر و فقط اگر الگوریتمی موجود باشد که فقط روی ورودی‌هایی که عضو A هستند متوقف شود. به عبارت دیگر این الگوریتم (تک‌ورودی) فقط وقتی روی $x \in \Sigma^*$ متوقف می‌شود که $x \in A$.

تعریف ۶.۱.۱. (ترم [۳۴]). ترم‌های یک زبان $\mathcal{L}$ ($\mathcal{L}$-ترم‌ها) به صورت استقرایی زیر تعریف می‌شوند:

(الف) هر متغیر و هر نماد ثابت $\mathcal{L}$، یک $\mathcal{L}$-ترم است.

(ب) اگر $t_1, ..., t_n$، $\mathcal{L}$-ترم باشند و f یک نماد تابعی n-موضعی $\mathcal{L}$ باشد، آنگاه عبارت $f(t_1, ..., t_n)$ یک $\mathcal{L}$- ترم است.

تعریف ۷.۱.۱. (فرمول‌های اتمی [۳۴]). فرمول‌های اتمی یک زبان مرتبه اول $\mathcal{L}$، عبارت‌هایی به شکل $R(t_1, ..., t_n)$ هستند، که در آن R یک نماد محمولی n-موضعی $\mathcal{L}$ است و $t_1, ..., t_n$، $\mathcal{L}$-ترم هستند.

تعریف ۸.۱.۱. (فرمول مرتبه اول [۳۴]). فرمول‌های یک زبان مرتبه اول $\mathcal{L}$ ($\mathcal{L}$-فرمول‌ها) به صورت بازگشتی تعریف می‌شود:

(الف) هر فرمول اتمی $\mathcal{L}$، یک $\mathcal{L}$-فرمول است.

(ب) اگر φ و ψ دو $\mathcal{L}$-فرمول باشند، آنگاه موارد زیر نیز $\mathcal{L}$-فرمولند:

$$(\neg\varphi)، (\varphi \wedge \psi)، (\varphi \vee \psi)، (\varphi \to \psi)، (\varphi \leftrightarrow \psi)، \big((\forall x_i)\varphi\big)، \big((\exists x_i)\varphi\big).$$

[۱] یک الگوریتم عبارت است از یک مجموعه‌ی کارآمد صریح از دستورالعمل‌هایی برای یک شیوه محاسباتی (که لزوماً عددی نیست) و ممکن است برای یافتن جواب‌های رده‌ی مفروضی از سوالات به کار رود.

تعریف ۹.۱.۱. (جمله [۳۴]). یک $\mathcal{L}$-فرمول مرتبه اول را $\mathcal{L}$-جمله نامیم هرگاه هیچ متغیر آزادی[۱] نداشته باشد.

تعریف ۱۰.۱.۱. مجموعه Δ_0 متشکل از تمام فرمول‌های حسابی است که سورهای موجود در آن‌ها همگی محدود[۲] هستند. فرض کنید $\varphi \in \Delta_0$؛ در این صورت فرمول $\forall x_0 \forall x_1 ... \forall x_n \varphi$ یک Π_1-فرمول و فرمول $\exists x_0 \exists x_1 ... \exists x_n \varphi$ یک Σ_1-فرمول است.

تعریف ۱۱.۱.۱. (نظریه [۱۳]). یک مجموعه از $\mathcal{L}$-جمله‌ها مثل $\mathbf{T}$ را نظریه گوییم هرگاه تحت استنتاج بسته باشد، یعنی برای هر $\mathcal{L}$-جمله‌ی φ، اگر $\mathbf{T} \vdash \varphi$، آنگاه $\varphi \in \mathbf{T}$.

تعریف ۱۲.۱.۱. (نظریه صحیح[۳] [۲۷]). نظریه‌ی $\mathbf{T}$، نظریه صحیح گفته می‌شود اگر و فقط اگر تمام قضیه‌های آن (در مدل استاندارد حساب) درست باشد.

مثال ۱۳.۱.۱. حساب پئانو که در ادامه تعریف خواهیم کرد یک نظریه‌ی صحیح است.

تعریف ۱۴.۱.۱. (نظریه سازگار[۴] [۲۷]). نظریه‌ی $\mathbf{T}$ را سازگار گویند هرگاه هیچ تناقضی را اثبات نکند. به عبارت دیگر، هیچ فرمول φ‌ای وجود نداشته باشد به طوری که برای آن هر دو $\mathbf{T} \vdash \varphi$ و $\mathbf{T} \vdash \neg\varphi$ برقرار باشند. در غیر اینصورت نظریه را ناسازگار[۵] گویند.

ملاحظه ۱۵.۱.۱. *هر نظریه صوری صحیح، سازگار است. زیرا اگر T یک نظریه صحیح باشد آنگاه برای هر $\mathcal{L}$-جمله‌ی φ، $\mathbf{T}$ نمی‌تواند هم φ و هم $\neg\varphi$ را ثابت کند، چون از آنجایی که هم φ و هم $\neg\varphi$ نمی‌توانند هم‌زمان در مدل استاندارد حساب درست باشند لذا با توجه به تعریف نظریه‌ی صحیح نمی‌توانند در $\mathbf{T}$ هم اثبات شوند. پس در نتیجه $\mathbf{T}$ سازگار است.*

---

[۱] گوییم x_i یک متغیر آزاد $\mathcal{L}$-فرمول φ است هرگاه x_i حداقل در یکی از دامنه عمل سورهای φ قرار نداشته باشد (حداقل محدود به یکی از سورها نباشد).

[۲] یک $\mathcal{L}$-فرمول φ با سور محدود گفته می‌شود هرگاه به شکل $\forall x < t\ \psi(x)$ یا $\exists x < t\ \psi(x)$ باشد که در آن ψ یک $\mathcal{L}$-فرمول بدون سور و t یک عدد است. برای مثال $\forall x < 5\ \ 2^x < 17$ یک فرمول با سور محدود است.

[۳] Sound

[۴] Consistent

[۵] Inconsistent

تعریف ۱.۱.۱۶. (نظریه اصل‌پذیر [۱۳]). نظریه‌ی $\mathbf{T}$ به طور بازگشتی اصل‌پذیر، یا به اختصار اصل‌پذیر، گفته می‌شود اگر و تنها اگر یک مجموعه‌ی تصمیم‌پذیر از $\mathcal{L}$-جمله‌ها مانند Σ وجود داشته باشد به طوری که $\mathbf{T} = Cn(\Sigma)$ که در آن $Cn(\Sigma)$ مجموعه‌ی همه‌ی $\mathcal{L}$-جمله‌هایی است که نتیجه‌ی منطقی Σ هستند را نشان می‌دهد، یعنی $Cn(\Sigma) = \{\sigma \ : \ \Sigma \vDash \sigma\}$.

تعریف ۱.۱.۱۷. (توسیع نظریه [۱۴]). $\mathbf{T}$ را یک نظریه در نظر بگیرید. یک توسیع از $\mathbf{T}$ نظریه صوری است که بتواند تمامی قضایای $\mathbf{T}$ را ثابت کند.

تبصره ۱.۱.۱۸. یک نظریه صوری می‌تواند توسیعی از $\mathbf{T}$ باشد ولی هیچ یک از اصول موضوعه آن با $\mathbf{T}$ مشترک نباشد.

مثال ۱.۱.۱۹. دو نظریه‌ی $\mathbf{T}$ و $\mathbf{S}$ را به صورت زیر در نظر بگیرید:

$$\mathbf{T} = \{\neg\forall x P(x), \forall x[\neg Q(x) \to P(x)]\} \text{ و}$$
$$\mathbf{S} = \{\exists x[\neg P(x) \wedge Q(x)], \neg\exists x[\neg P(x) \wedge \neg Q(x)]\}.$$

به وضوح $\mathbf{T} \cap \mathbf{S} = \emptyset$. حال نشان می‌دهیم که $\mathbf{T} \equiv \mathbf{S}$. برای این منظور، نشان می‌دهیم که هر مدل $\mathbf{T}$ مدلی برای $\mathbf{S}$ است و برعکس. ابتدا نشان می‌دهیم که هر مدل $\mathbf{T}$ مدلی برای $\mathbf{S}$ است. اگر $\mathbf{T}$ مدل نداشته باشد آنگاه حکم به انتفای مقدم برقرار است. پس فرض می‌کنیم $\mathcal{M}$ با مجموعه زمینه‌ی M مدلی برای $\mathbf{T}$ باشد. در این صورت $\mathcal{M} \models \mathbf{T}$، بنابراین $\mathcal{M} \models \neg\forall x P(x)$ و $\mathcal{M} \models \forall x[\neg Q(x) \to P(x)]$. از آنجایی که $\mathcal{M} \models \neg\forall x P(x)$، داریم $\mathcal{M} \not\models \forall x P(x)$ و این نشان می‌دهد که به ازای یک $\bar{a} \in M$، $\mathcal{M} \models \neg P(\bar{a})$(*). و از آنجایی که $\mathcal{M} \models \forall x[\neg Q(x) \to P(x)]$، می‌توان گفت که برای هر $\bar{b} \in M$، $\mathcal{M} \models \neg Q(\bar{b}) \to P(\bar{b})$. از اینرو، برای هر $\bar{b} \in M$، اگر $\mathcal{M} \models \neg Q(\bar{b})$ آنگاه $\mathcal{M} \models P(\bar{b})$(**). یک $\bar{a}$ را که در رابطه (*) صدق می‌کند را انتخاب می‌کنیم، پس $\mathcal{M} \models \neg P(\bar{a})$ یا معادلا $\mathcal{M} \not\models P(\bar{a})$. حال برای این $\bar{a}$ از رابطه‌ی (**) نتیجه می‌شود که $\mathcal{M} \not\models \neg Q(\bar{a})$ یا معادلا $\mathcal{M} \models Q(\bar{a})$. پس به ازای یک $\bar{a} \in M$ داریم $\mathcal{M} \models \neg P(\bar{a})$ و $\mathcal{M} \models Q(\bar{a})$؛ لذا به ازای همان $\bar{a} \in M$ داریم $\mathcal{M} \models \neg P(\bar{a}) \wedge Q(\bar{a})$، و این بدین معنی است که $\mathcal{M} \models \exists x[\neg P(x) \wedge Q(x)]$. حال نشان می‌هیم که $\mathcal{M} \models \neg\exists x[\neg P(x) \wedge \neg Q(x)]$ یا معادلا

$\mathcal{M} \not\models \exists x[\neg P(x) \wedge \neg Q(x)]$. از آنجایی که $\mathcal{M} \not\models \exists x[\neg P(x) \wedge \neg Q(x)]$ معادل با این است که برای هر $\bar{a} \in M$، $\mathcal{M} \not\models \neg P(\bar{a}) \wedge \neg Q(\bar{a})$ و این معادل با $\mathcal{M} \not\models \neg P(\bar{a})$ یا $\mathcal{M} \not\models \neg Q(\bar{a})$ است که این خود نیز با $\mathcal{M} \models P(\bar{a})$ یا $\mathcal{M} \models Q(\bar{a})$ معادل است، لذا کافی است نشان دهیم که برای هر $\bar{a} \in M$، $\mathcal{M} \models P(\bar{a}) \vee Q(\bar{a})$. چون $\mathcal{M} \models \forall x[\neg Q(x) \to P(x)]$، بنابراین برای هر $\bar{a} \in M$، $\mathcal{M} \models \neg Q(\bar{a}) \to P(\bar{a})$؛ پس برای هر $\bar{a} \in M$، اگر $\mathcal{M} \models \neg Q(\bar{a})$ آنگاه $\mathcal{M} \models P(\bar{a})$، یا معادلا برای هر $\bar{a} \in M$، $\mathcal{M} \not\models \neg Q(\bar{a})$ یا $\mathcal{M} \models P(\bar{a})$، لذا برای هر $\bar{a} \in M$، $\mathcal{M} \models Q(\bar{a})$ یا $\mathcal{M} \models P(\bar{a})$، پس برای هر $\bar{a} \in M$، $\mathcal{M} \models P(\bar{a}) \vee Q(\bar{a})$. و درنتیجه با توجه به توضیحات فوق $\mathcal{M} \models \neg\exists x[\neg P(x) \wedge \neg Q(x)]$. حال نشان می‌دهیم که هر مدل **S** مدلی برای **T** است. اگر **S** مدل نداشته باشد حکم به انتفای مقدم برقرار است. فرض کنیم که $\mathcal{N}$ با مجموعه زمینه‌ی N مدلی برای **S** باشد، لذا $\mathcal{N} \models \exists x[\neg P(x) \wedge Q(x)]$ و $\mathcal{N} \models \neg\exists x[\neg P(x) \wedge \neg Q(x)]$. چون $\mathcal{N} \models \exists x[\neg P(x) \wedge Q(x)]$ همانند توضیحات فوق برای هر $\bar{a} \in N$، $\mathcal{N} \models P(\bar{a}) \vee Q(\bar{a})$. پس برای هر $\bar{a} \in N$، اگر $\mathcal{N} \models \neg Q(\bar{a})$، آنگاه $\mathcal{N} \models P(\bar{a})$، و بنابراین $\mathcal{N} \models \neg Q(\bar{a}) \to P(\bar{a})$. در نتیجه $\mathcal{N} \models \forall x[\neg Q(x) \to P(x)]$. و از آنجایی که $\mathcal{N} \models \exists x[\neg P(x) \wedge Q(x)]$، می‌توان گفت به ازای یک $\bar{a} \in N$، $\mathcal{N} \models \neg P(\bar{a}) \wedge Q(\bar{a})$، بنابراین به ازای یک $\bar{a} \in N$، $\mathcal{N} \models \neg P(\bar{a})$ و هم $\mathcal{N} \models Q(\bar{a})$. از اینرو به ازای یک $\bar{a} \in N$، $\mathcal{N} \models \neg P(\bar{a})$ یا معادلا $\mathcal{N} \not\models P(\bar{a})$، و این یعنی $\mathcal{N} \not\models \forall x P(x)$ یا معادلا $\mathcal{N} \models \neg\forall x P(x)$. پس $\mathbf{T} \equiv \mathbf{S}$.

۲.۱ حساب مرتبه اول

تعریف ۱.۲.۱. (حساب پئانو [۲۹]). $\mathcal{L}_A = \{+, \cdot, S, <, 0, 1\}$ را به عنوان زبان اعداد طبیعی، که در آن تابع S نشان دهنده تابع تالی است، $S(x) = x + 1$، در نظر بگیرید. نظریه **Q** را با اصول زیر مشخص می‌کنیم:

1. $\forall x \neg\big(S(x) = 0\big)$
2. $\forall x \forall y\big(S(x) = S(y) \longrightarrow x = y\big)$

3. $\forall x\big(x + 0 = x\big)$

4. $\forall x \forall y\big(x + S(y) = S(x + y)\big)$

5. $\forall x\big(x \cdot 0 = 0\big)$

6. $\forall x \forall y\big(x \cdot S(y) = x \cdot y + x\big)$

7. $\forall x\big[\neg(x < 0)\big]$

8. $\forall x \forall y\big(x < S(y) \longleftrightarrow x < y \vee x = y\big)$

9. $\forall x \forall y\big(x < y \vee y < x \vee x = y\big).$

اگر به نظریه فوق، مجموعه اصول زیر را برای هر $\mathcal{L}$-فرمول φ، بیافزاییم، نظریه جدیدی حاصل می‌شود که ما آن را حساب پئانو می‌نامیم و با **PA** نشان می‌دهیم.

10. $\varphi(0) \wedge \forall x\big[\varphi(x) \longrightarrow \varphi\big(S(x)\big)\big] \longrightarrow \forall x \varphi(x).$

اصول فوق، استقراء نام دارند.

توجه داشته باشید که اعداد طبیعی، $\mathbb{N}$، همراه با عمل جمع، ضرب و رابطه‌ی کوچک‌تری معمولی، مدلی برای نظریه‌ی **PA** می‌باشد که مدل استاندارد **PA** نامیده می‌شود.

قضیه ۲.۲.۱. ([۳۴]). *نظریه* **Q**، *Σ_1-جمله‌های درست در $\mathbb{N}$ را ثابت می‌کند.*

تعریف ۳.۲.۱. (تابع تام [۲۷]). تابع $f : A \longrightarrow B$ را تابع تام گوییم هرگاه روی تمام اعضای A تعریف شده باشد. یعنی به ازای هر $x \in A$، $f(x) \in B$ باشد.
در غیر اینصورت تابع f را تابع جزیی می‌نامیم.

تعریف ۴.۲.۱. (تابع Σ_1-تعریف‌پذیر در PA [۳۴]). تابع $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ را Σ_1-تعریف‌پذیر در **PA** گوییم هرگاه Σ_1-فرمولی مانند φ در **PA** وجود داشته باشد به طوری که

۱. $\mathbf{PA} \vdash \forall \overline{x}\ \exists! y\ \ \varphi(\overline{x}, y)$ و

۲. برای $m \in \mathbb{N}$ و $\overline{k} \in \mathbb{N}^n$ اگر $f(\overline{k}) = m$ باشد آنگاه $\mathbf{PA} \vdash \varphi(\overline{k}, m)$.

تعریف ۵.۲.۱. (تابع محاسبه‌پذیر [۱۵]). تابع $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ را محاسبه‌پذیر گوییم هرگاه به طور استقرایی زیر بدست آمده باشد:

(الف) توابع جمع، ضرب و توابع تصویر محاسبه‌پذیرند.

(ب) اگر $G : \mathbb{N}^m \longrightarrow \mathbb{N}$ و $H_1, ..., H_m : \mathbb{N}^n \longrightarrow \mathbb{N}$ توابع محاسبه‌پذیر باشند، آنگاه تابع $F : \mathbb{N}^n \longrightarrow \mathbb{N}$ که برای $\overline{a} = (a_0, ..., a_n) \in \mathbb{N}^n$ به صورت زیر تعریف می‌شود نیز محاسبه‌پذیر است:

$$.F(\overline{a}) = G\big(H_1(\overline{a}), ..., H_m(\overline{a})\big)$$

(پ) اگر $G : \mathbb{N}^{n+1} \longrightarrow \mathbb{N}$ محاسبه‌پذیر و برای هر $\overline{a} = (a_0, ..., a_n) \in \mathbb{N}^n$، $x \in \mathbb{N}$ موجود باشد که $G(\overline{a}, x) = 0$، آنگاه تابع $F : \mathbb{N}^n \longrightarrow \mathbb{N}$ با تعریف زیر محاسبه پذیر (و تام) است:

$$.F(\overline{a}) = \mu x\big(G(\overline{a}, x) = 0\big)$$ [۱]

ملاحظه ۶.۲.۱. *توجه داشته باشید که اگر در بند (پ) تعریف فوق، شرط «برای هر $\overline{a} \in \mathbb{N}^n$، $x \in \mathbb{N}$ موجود باشد که ...» را حذف کنیم، آنگاه تعریف تابع جزیی محاسبه‌پذیر را خواهیم داشت.*

۳.۱ قضیه اول ناتمامیت

در سال ۱۹۳۱ کورت گودل[۲] قضایای معروف ناتمامیت اول و دوم را ثابت کرد و دنیای ریاضی را متحول ساخت. در حقیقت قضایای ناتمامیت گودل[۳] نشان می‌دهند که نظریه‌ای سازگار در شاخه‌های به اندازه قوی از ریاضیات منجر به یافتن گزاره‌های تصمیم‌ناپذیر می‌شود که یک پاسخ منفی به دومین مسئله هیلبرت[۴] در رابطه با «آیا ریاضیات علمی کامل است؟» در نظر گرفته می‌شود. گودل در مقاله معروف خود قضیه اول ناتمامیت خود را به صورت زیر بیان کرد:

[۱] $\mu x\big(G(\overline{a}, x) = 0\big)$ نشان دهنده کوچکترین x است که در خاصیت $G(\overline{a}, x) = 0$ صدق می‌کند.

[۲] K. Gödel

[۳] Gödel's Incompleteness Theorems

[۴] D. Hilbert

قضیه ۱.۳.۱. (***قضیه اول ناتمامیت گودل*** **[۳۴]**). *برای هر نظریه سازگار ریاضی به اندازه کافی غنی مانند* **PA** *یا* **ZFC**، *جمله‌ای وجود دارد که نه خودش اثبات‌پذیر است و نه نقیض آن. به عبارت دیگر، برای هر نظریه سازگار ریاضی به اندازه کافی غنی مانند* **PA** *یا* **ZFC**، *جمله‌ای وجود دارد که درست است ولی اثبات‌پذیر نیست.*

۴.۱ مبانی نظریه محاسبه‌پذیری

در سال ۱۹۳۶ تورینگ[۵] نوع بسیار ساده‌ای از ماشین‌های فرضی را نمایش داده و برهان درخشانی درباره‌ی اینکه هر چیزی که بتواند به صورت معقول توسط محاسبات انسانی با روش معینی محاسبه شود می‌تواند توسط یک چنین ماشینی محاسبه شود، ارایه کرد. همچنان که تورینگ ادعا کرده بود، هر پردازشی که بتواند به طور طبیعی «روش مؤثر» نامیده شود توسط یک ماشین تورینگ محقق می‌شود. این ادعا تحت عنوان فرضیه تورینگ[۶] مطرح می‌شود. در چند سال گذشته، تلاش‌های جدی برای ارایه تعریف رضایت‌بخشِ دقیق و در عین حال محسوسِ مفهوم «روش مؤثر»، نتیجه معادل را در مفهوم گسترده‌تر که در اصل همان تعریف کلاس پردازش‌ها است در پی داشته است. (تورینگ در مقاله‌ی اصلیش بین مفهوم «روش مؤثر» خودش با مفهوم «قابلیت شمارش کارآمد» چرچ[۷] هم‌ارزی ایجاد می‌کند.) فرضیه چرچ[۸] این مفهوم را بیان می‌کند که، صرف نظر از یک صوری‌سازی دقیق، یک مفهوم واقعی از محاسبه‌پذیری مؤثر وجود دارد.

[۵] A. Turing

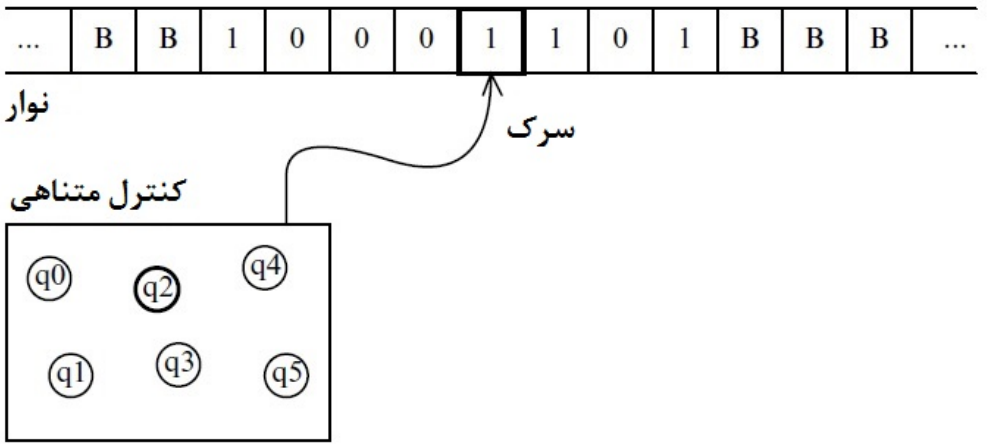
[۶] Turing's Thesis

[۷] A. Church

[۸] Church's Thesis

۱.۴.۱ شمارش‌های کارآمد و ماشین‌های جهانی

ماشین تورینگ را به شکل زیر صوری‌سازی می‌کنیم: یک ماشین تورینگ شامل یک برنامه متناهی (که کنترل متناهی نامیده می‌شود) که با استفاده از نشانگر دسترسی (که سَرَک[۹] نامیده می‌شود) قادر به دستکاری یک فهرست خطی از سلول‌هاست (که نوار نامیده می‌شود) می‌باشد. ما به دو جهت تحت عنوان حرکت به راست (R) و حرکت به چپ (L) روی نوار حرکت می‌کنیم. کنترل متناهی می‌تواند روی هر یک از اعضای مجموعه‌ی متناهی از حالت‌های S_M قرار گیرد، و سلول نوار می‌تواند شامل یک 0، یک 1 و یا یک فضای خالی B باشد. زمان گسسته و لحظات زمان به ترتیب $0, 1, 2, \ldots$ می‌باشند و 0 در هر ماشین لحظه‌ی شروع محاسباتش است. در هر لحظه، سرک روی سلول خاص قرار می‌گیرد، که به آن اسکن گفته می‌شود. سرک در لحظه 0 روی سلول مشخصی روی نوار قرار می‌گیرد که به آن سلول شروع می‌گویند، و کنترل متناهی نیز روی حالت مشخص q_0 قرار می‌گیرد. در لحظه‌ی 0، تمام سلول‌های نوار، به جز تعداد متناهی از سلول‌ها که از سلول شروع به سمت راست شامل 0 و 1 هستند، شامل نماد B می‌باشند. این رشته‌ی دودویی ورودی نام دارد.



شکل ۱ ماشین تورینگ

دستگاه می‌تواند توسط عملگرهای پایه‌ای زیر اجرا شود:

[۹] Head

۱. می‌تواند عضوی از $\Gamma = \{0, 1, B\}$ را روی سلولی که اسکن می‌شود بنویسد، و یا

۲. می‌تواند سرک را روی سلول به سمت راست یا چپ انتقال دهد.

چون دستگاه فعال است، این عملیات را در هر مرحله تکرار می‌کند. در محاسبه هر مرحله، کنترل متناهی حالتی از S_M را می‌گیرد. دستگاه به گونه‌ای ساخته شده است که مطابق با فهرستی از قوانین عمل می‌کند. این قوانین، حالت فعلی کنترل متناهی و نمادی که سلول تحت اسکن شامل آن است را تعیین می‌کند، عملیات مرحله بعد را اجرا کرده و حالت را در پایان اجرای عملیات بعد وارد می‌کند. قواعد به شکل (p, s, a, q) می‌باشند که در آن p حالت فعلی کنترل متناهی، s نمادی که سلول تحت اسکن دارد، a عملیات مرحله بعد است که به شکل (۱) یا (۲) توسط عضوی از $S = \{0, 1, B, L, R\}$ اجرا شده است، و q حالتی از کنترل متناهی است که در پایان این مرحله وارد می‌شود. دو چهارتایی متمایز نمی‌توانند عضوهای ابتدایی یکسانی داشته باشند، و این یعنی دستگاه قطعی است. همه‌ی ترکیب‌های ممکن از دو عضو ابتدایی لازم نیست در مجموعه باشد؛ در اینصورت اجازه می‌دهیم دستگاه هیچ عملیاتی انجام ندهد. در این حالت می‌گوییم دستگاه متوقف شده است. بنابراین، ما می‌توانیم یک ماشین تورینگ را توسط تابعی از یک زیرمجموعه متناهی از $S_M \times \Gamma$ به $S_M \times \Gamma \times \{L, R, S\}$ تعریف کنیم. برای یک ماشین تورینگ و یک ورودی داده شده، ماشین تورینگ یک سلسله منحصر به فرد از عملیات‌های تعیین شده را اجرا می‌کند، که ممکن است در یک تعداد متناهی از مراحل به پایان برسد یا نرسد.

ما می‌توانیم یک تابع جزیی را به صورت زیر به یک ماشین تورینگ نسبت دهیم: ورودی ماشین تورینگ به عنوان یک nتایی $(x_1, ..., x_n)$ از رشته‌های دودویی به شکل رشته‌ی دودویی منحصر به فرد متشکل از نسخه‌ی خود مرزبند[۱] x_iها است. عدد نشان داده شده توسط حداکثر رشته‌ی دودویی (مرزبندی شده توسط فضای خالی) است که از تعدادی بیت اسکن شده، یا اگر یک فضای خالی اسکن شده باشد 0 است، با لحظه‌ای که ماشین متوقف می‌شود، خروجی محاسبه نامیده می‌شود.

تعریف ۱.۴.۱. (تابع بازگشتی جزیی [۲۷]). هر ماشین تورینگ یک تابع جزیی از $\mathbb{N}^n$ به $\mathbb{N}$، به

[۱] اگر $l(x)$ را طول رشته‌ی دودویی x در نظر بگیریم (برای مثال، اگر $x = x_1x_2...x_n$ باشد آنگاه $l(x) = n$)، آنگاه نسخه‌ی خود مرزبند x را با $\overline{x}$ نشان داده و به صورت زیر تعریف می‌کنیم: $\overline{x} = 1^{l(x)}0x$. برای مثال، اگر $x = 110$ باشد، آنگاه $\overline{x} = 1110110$.

ازای $n \geqslant 1$، را تعریف می‌کند که ما چنین تابعی را یک تابع بازگشتی جزیی می‌نامیم. اگر ماشین تورینگ برای همه‌ی ورودی ها متوقف شود، آنگاه محاسبه‌ی تابع برای تمام دامنه تعریف شده و در این صورت تابع را تابع بازگشتی تام یا به اختصار بازگشتی گوییم.

مثال ۲.۴.۱. x را به عنوان یک رشته‌ی دودویی درنظر بگیرید. نشان دادن تابع بازگشتی جزیی بودن توابع $l(x)$، $f(x) = \overline{x}$، $g(\overline{x}y) = x$ و $h(\overline{x}y) = y$ آسان است. اما توابع g و h تام نیستند زیرا برای ورودی 1111 تعریف نشده‌اند.

مثال ۳.۴.۱. تابع $\langle x, y\rangle = \overline{x}y$ از $\mathbb{N} \times \mathbb{N}$ به $\mathbb{N}$، تابع بازگشتی تام یک به یک است. ما می‌توانیم به سادگی این روند را برای به دست آوردن تابع بازگشتی تام یک به یک از $\mathcal{N}^k$ به $\mathcal{N}$، برای هر ثابت k، توسعه داده و به شکل $\langle n_1, n_2, ..., n_k\rangle = \langle n_1, \langle n_2, ..., n_k\rangle\rangle$ تعریف کنیم.

۲.۴.۱ ماشین‌های تورینگ

تعریف ۴.۴.۱. (ماشین تورینگ [۲۸]). هر ماشین تورینگ مانند M با یک شش تایی به شکل $M = (S_M, \Gamma, \Sigma, \delta_M, I_M, F_M)$ تعریف می‌شود که در آن:

۱. S_M مجموعه حالت‌های M است،

۲. Γ مجموعه متناهی از علائم که الفبای نوار نامیده می‌شود به علاوه‌ی عضو شاخص B که نشان دهنده‌ی نماد خالی است،

۳. Σ الفبای ورودی است ($\Sigma \subseteq \Gamma \setminus \{B\}$)،

۴. δ_M تابع انتقال است که به صورت تابع جزئی زیر تعریف می‌شود:

$$\delta_M : (S_M - F_M) \times \Gamma \longrightarrow S_M \times \Gamma \times \{L, R, S\}$$

که در آن R حرکت به راست، L حرکت به چپ و S سکون است،

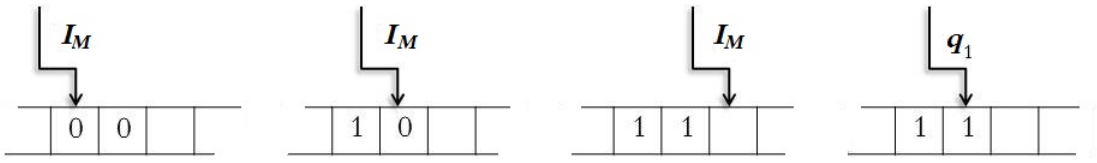
۵. $I_M \in S_M$ حالت اولیه و

۶. $F_M \subseteq S_M$ مجموعه حالت‌های نهایی ماشین تورینگ می‌باشد.

در تعریف فوق تفسیر تابع δ_M نحوه عملکرد ماشین تورینگ را روشن می‌کند. در حقیقت تابع روی دوتایی حالت فعلی واحد کنترل و نماد فعلی که از نوار خوانده می‌شود اثر می‌گذارد و سه تایی متشکل از یک حالت جدید در واحد کنترل، یک نماد جدید روی نوار که جایگزین نماد قبلی می‌شود و حرکت به سمت چپ، راست یا سکون می‌باشد.

با مثال زیر [۲۸] عملکرد ماشین تورینگ ساده‌ای را تا حدی نشان می‌دهیم.

مثال ۵.۴.۱. ماشین تورینگ زیر را در نظر بگیرید:



شکل ۲ دنباله‌ای از حرکت‌ها

که در آن $S_M = \{I_M, q_1\}$، $\Sigma = \{0, 1\}$، $\Gamma = \{0, 1, B\}$، $F_M = \{q_1\}$، $\delta_M(I_M, 0) = (I_M, 1, R)$، $\delta_M(I_M, 1) = (I_M, 1, R)$ و $\delta_M(I_M, B) = (q_1, B, L)$ هستند. اگر این ماشین تورینگ در حالت I_M با علامت 0 در زیر سَرَکِ خواندن و نوشتن شروع کند، ماشین تابع انتقال را به صورت $\delta_M(I_M, 0) = (I_M, 1, R)$ اعمال می‌کند. بنابراین سَرَک 0 را با 1 جایگزین کرده و روی نوار به سمت راست حرکت می‌کند و ماشین در حالت I_M باقی می‌ماند. به همین ترتیب 0های بعدی روی نوار با 1 جایگزین می‌شوند اما 1ها تغییر نمی‌کنند. در پایان وقتی که ماشین به اولین سلول خالی برسد یک سلول به چپ برگشته و در حالت نهایی q_1 متوقف می‌شود. شکل ۲ چند مرحله از این پردازش را نشان می‌دهد.

هر ماشین تورینگ به وسیله تابع انتقال منحصر به فردش مشخص می‌شود. با یک کدگذاری مناسب می‌توان اعداد رمز را به تابع‌های انتقال تخصیص داد (به تعریف ۷.۴.۱ مراجعه کنید).

بنابراین می‌توان به هر ماشین تورینگ یک عدد رمز مختص کرد. با توجه به این توضیحات می‌توان گفت که مجموعه‌ی همه‌ی ماشین‌های تورینگ را می‌توان به صورت $\Phi_1, \Phi_2, ...$ فهرست کرد به طوری که هر اندیسی به طور کارآمد و کامل دستورالعمل‌های ماشین تورینگ متناظر را مشخص کند. توضیحات فوق به تعریف شمارش کارآمد ماشین‌های تورینگ منجر می‌شود [۱۴].

تعریف ۶.۴.۱. تابع یک به یک کارآمدی که بین اعداد طبیعی و ماشین‌های تورینگ، با توجه به توضیحات فوق الذکر، معرفی می‌کنیم، شمارش کارآمد ماشین‌های تورینگ نامیده می‌شود.

حال مفهوم ماشین تورینگ را در **PA** فرمول‌بندی می‌کنیم.

تعریف ۷.۴.۱. فرض کنید سلول‌های نوار از سلول شروع به سمت راست با $0, 1, 2, ...$ شماره‌گذاری شده باشد.

۱. ما انتقال ماشین تورینگ M را با یک چندتایی به شکل

$$\langle q, s, q', s', m \rangle$$

کدگذاری می‌کنیم که در آن $m \in \{L, R, S\}$. δ_M دستوری است که اگر ماشین در حالت q روی سلول با نماد s باشد، به حالت q' انتقال یابد و در سلول s' را نوشته و به چپ (L) یا راست (R) حرکت کند و یا بایستد (S).

۲. یک ماشین تورینگ M توسط عدد دنباله‌ای

$$\langle N_{S_M}, \delta, I_M, l_F \rangle$$

کدگذاری می‌شود، به طوری که در آن N_{S_M} تعداد حالات M می‌باشد و I_M حالت اولیه M است به طوری که $I_M < N_{S_M}$ می‌باشد؛ l_F یک عدد دنباله‌ای است که مجموعه حالات نهایی را کدگذاری می‌کند، و δ یک عدد دنباله‌ای است که مجموعه انتقال‌ها را کدگذاری می‌کند.

۳. یک توصیف لحظه‌ای[۲]، یا یک ID، توسط عدد دنباله‌ای

$$\langle q, t, h\rangle$$

کدگذاری می‌شود، به طوری که $q < N_{S_M}$ کد یک حالت است، t یک عدد دنباله‌ای است که محتوای یک دنباله متناهی پیوسته از سلول‌های شامل نمادهای غیر تهی ظاهر شده روی نوار را کدگذاری می‌کند، و h موقعیت سَرَک است.

۴. یک پردازش از M با عدد دنباله‌ای

$$\langle ID_0, ID_1, ..., ID_l\rangle$$

از توصیف‌های لحظه‌ای کدگذاری می‌شود به طوری که در آن ID_0 حالت اولیه، و برای هر $i < n$، ID_{i+1} توسط δ_M از ID_i به دست می‌آید.

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 پردازشی از ماشین تورینگ کدگذاری شده با m 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 $x_0 = a_0$، برای $i = 1, ..., n$، $x_i = 2x_{i-1} + a_i$ و $x = x_n$.

بنابراین، Σ_1-فرمول $bin(x, t)$ موجود است که می‌گوید «t عدد دنباله‌ای است که نمایش دودویی x را کدگذاری می‌کند». بنابراین یک Σ_1-فرمول مانند $\Psi_1(m, y, z)$ داریم که بیان می‌کند

[۲] Instantaneous Descriptions

«z یک ID از ماشین تورینگ کدگذاری شده با m و محتویات نوار، نمایش دودویی عدد y است». با استفاده از این فرمول، Σ_1-فرمول $\Psi_2(p,m,x)$ را می‌توان تعریف کرد که بیان می‌کند «p عدد دنباله‌ای یک دنباله معتبر از IDهای ماشین تورینگی که کد آن m است را نشان می‌دهد به طوری که نمایش دودویی عدد x (در ابتدای محاسبه) بر روی نوار آن ماشین تورینگ نوشته شده است». 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 (برای درک بیشتر به [۱۴] مراجعه شود). پس عبارت «$\Phi_m(x)=y$» یا «$\Phi_m(x)\downarrow y$» را می‌توان با فرمول زیر نوشت

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

هر شمارش کارآمد از ماشین‌های تورینگ $\Phi_1,\Phi_2,\ldots$، یک شمارش کارآمد از توابع بازگشتی جزیی $\phi_1,\phi_2,\ldots$ را تعیین می‌کند به طوری که تابع بازگشتی جزیی ϕ_i توسط ماشین تورینگ Φ_i محاسبه شده است. این مهم است که بین یک تابع ψ و یک نام برای ψ فرق گذاشته شود. یک نام برای ψ می‌تواند الگوریتمی باشد که به شکل یک ماشین تورینگ Φ، ψ را محاسبه می‌کند. آن می‌تواند عدد طبیعی iای باشد به طوری که در فهرست فوق ψ معادل ϕ_i باشد. ما این عدد طبیعی i را اندیسی برای ψ می‌نامیم. بنابراین، هر تابع بازگشتی جزیی ψ ممکن است چندین بار در شمارش کارآمد توابع بازگشتی جزیی ظاهر شده باشد، لذا تعداد زیادی اندیس دارد.

الگوریتم زیر را در نظر بگیرید: اگر زوج دلخواهی از اعداد مانند (m,n) داده شده باشد، فهرست $\Phi_1,\Phi_2,\ldots$ از ماشین‌های تورینگ را شمارش کنید تا Φ_m را بیابید، و n را به عنوان ورودی Φ_m به کار ببرید. این الگوریتمی است برای محاسبه‌ی تابع (جزیی) دو متغیره. پس بنابر نظریه تورینگ، ماشین تورینگی وجود دارد که مقادیر این تابع را محاسبه می‌کند. این مطلب را می‌توان تحت حقیقت زیر بیان کرد.

حقیقت ۸.۴.۱. (ماشین تورینگ جهانی [۱۴]). ماشین تورینگی مانند Φ وجود دارد که اگر به عنوان محاسبه کننده‌ی مقادیر تابع دو متغیره روی (m,n) تلقی شود، محاسبه‌ی ماشین تورینگ Φ_m را به ازای ورودی n انجام می‌دهد. ما این ماشین تورینگ Φ را ماشین تورینگ جهانی می‌نامیم.

تعریف ۹.۴.۱. (تابع بازگشتی جزیی جهانی). تابع $v^{(2)}(i,x)$ که توسط ماشین تورینگ جهانی Φ محاسبه شده است را تابع بازگشتی جزیی جهانی می‌نامیم.

۵.۱ تصمیم‌ناپذیری مسئله توقف

مقاله‌ی تورینگ، و بیشتر از آن مقاله‌ی گودل، که در آن چنین نتیجه‌ای برای اولین بار ظاهر شد، برای نشان دادن این که سوالات خوشتعریف معین در حوزه ریاضی نمی‌تواند توسط هر روش مؤثر برای پاسخ‌دهی سوالات حل و فصل شده باشد، مشهور است. یکی از این سوالات چنین مطرح می‌شود: «آیا محاسبات ماشین در نهایت با یک نتیجه معین پایان می‌یابد، و آیا محاسبات ماشین تا ابد بدون نتیجه مشخصی ادامه می‌یابد؟» این سوال گاهی مسئله توقف نامیده می‌شود. چون می‌توان تمام ماشین‌ها را به ماشین تورینگ جهانی U شبیه کرد، این سوال نمی‌تواند در مورد ماشین U، یا به طور کلی برای هر ماشین تورینگ جهانی منحصر به فرد، قطعی باشد. با توجه به فرضیه تورینگ، این بحث را در لم زیر رسمی می‌کنیم. $\phi_1, \phi_2, \ldots$ را شمارش استاندارد توابع بازگشتی جزیی در نظر بگیرید.

لم ۱.۵.۱. *هیچ تابع جزیی gای وجود ندارد که برای تمام x و yها،*

$$g(x,y) = \begin{cases} 1 & \text{اگر } \phi_x(y) \text{ تعریف شده باشد} \\ 0 & \text{در غیر اینصورت} \end{cases}. \qquad (۱.۱)$$

برهان. فرض خلف می‌کنیم و تابع بازگشتی جزیی ψ را به صورت $\psi(x) = 1$ تعریف می‌کنیم اگر $g(x,x) = 0$ باشد و در غیر اینصورت $\psi(x)$ را تعریف نشده در نظر می‌گیریم. (تعریف ψ با فرض بازگشتی تام نبودن g یک الگوریتم به دست می‌دهد، و ما می‌توانیم توسط فرضیه چرچ یا توسط تفسیری صریح، ماشین تورینگی برای محاسبه‌ی ψ بیابیم.) فرض کنید ψ اندیس y را در شمارش توابع بازگشتی جزیی داشته باشد، $\psi = \phi_y$. در اینصورت مطابق با تعریف ψ، $\phi_y(y)$ تعریف می‌شود اگر و تنها اگر $g(y,y) = 0$ باشد. اما این متناقض با فرض وجود g که در صورت لم بیان شده است می‌باشد. □

روشی که در برهان لم فوق از آن استفاده شد، قطری سازی[۳] نام دارد.

تعریف ۲.۵.۱. مجموعه‌ی $K_0 = \{\langle x, y\rangle : \phi_x(y) < \infty\}$ را مجموعه‌ی توقف می‌نامیم.

۶.۱ مبانی نظریه احتمال

حساب احتمالات، مدل‌های ریاضی حالات (تجربیات و مشاهدات) که در آن نتیجه قطعی نیست اما توسط پیشامدهای غیر مسلم قطعی شده است را مورد مطالعه قرار می‌دهد. مجموعه‌ی تمام نتایج ممکن فضای نمونه نامیده می‌شود که اغلب با S نشان می‌دهیم و منظور ما از پیشامد E زیرمجموعه‌ای از S می‌باشد. فضای نمونه S می‌تواند شمارا باشد، بدین معنی که میتواند متناهی یا شمارای نامتناهی باشد، و یا می‌تواند پیوسته باشد، بدین معنی که ناشمارای نامتناهی باشد.

مثال ۱.۶.۱. در پرتاب دو تاس، یکی سفید و یکی سیاه، یک فضای نمونه S شامل تمام زوج‌های (i, j)ای است که i و j به ترتیب عدد روی تاس سفید و j عدد روی تاس سیاه را نشان می‌دهد. اگر $A = \{(1,3),(2,2),(3,1)\}$ باشد، آنگاه A پیشامدی است که مجموع i و j برابر 4 است. اگر $B = \{(1,1),(1,2),(2,1)\}$ باشد، آنگاه B پیشامدی است که مجموع i و j کمتر از 4 است.

مشاهده می‌شود که احتمال p از یک پیشامد A حد ظاهری فراوانی نسبی نتایج در پیشامد A در نهایت یک دنباله از تکرارهای مستقل از آزمایش است. برای مثال، احتمال مربوط به A در مثال فوق برابر $\frac{1}{12}$ است.

۱.۶.۱ اصول کولموگروف

فرض کنید S نشان دهنده‌ی فضای نمونه باشد. آنچه که کولموگروف در سال ۱۹۳۳ رسمیت بخشید و به طور مرسوم از آن استفاده می‌کنند تحت اصول زیر بیان می‌شود:

(A۱) اگر A و B دو پیشامد باشند، آنگاه اشتراک $A \cap B$، اجتماع $A \cup B$ و تفاضل $A - B$ نیز پیشامد هستند.

[۳] Diagonalization

(A۲) فضای نمونه S یک پیشامد است و آن را پیشامد حتمی می‌نامیم. مجموعه تهی که با $\varnothing$ نشان می‌دهیم، یک پیشامد است و به آن پیشامد غیرممکن می‌گوییم.

(A۳) به هر پیشامد E یک عدد حقیقی نا منفی $P(E)$ را اختصاص می‌دهیم که به آن احتمال پیشامد E می‌گویند.

(A۴) $P(S) = 1$.

(A۵) اگر A و B جدا از هم، یعنی $A \cap B = \varnothing$، آنگاه $P(A \cup B) = P(A) + P(B)$.

(A۶) برای یک دنباله نزولی $A_1 \subset A_2 \subset ... \subset A_n \subset ...$ از پیشامدها با خاصیت $\bigcap_n A_n = \varnothing$، داریم $\lim_{n\to\infty} P(A_n) = 0$.

برای مجموعه‌ی متناهی A، تعداد اعضای A را با $\#A$ نشان می‌دهیم و اگر مجموعه پیشامدها متناهی باشد و $A \subseteq S$، آنگاه $P(A) = \frac{\#A}{\#S}$. برای سیستم‌هایی که تعداد متناهی پیشامد دارند، اصل A۶ به وضوح از اصل‌های A۱ تا A۵ به دست می‌آید. اما برای سیستم‌هایی که تعداد نامتناهی پیشامد دارند، اصل A۶ مستقل از پنج اصل اول است. بنابراین، اصل A۶ فقط برای سیستم‌هایی که تعداد نامتناهی پیشامد دارند ضروری است.

یک سیستم $\mathcal{F}$ از مجموعه‌های $f \subseteq S$ که تحت عملگرهای دوتایی اجتماع، اشتراک و تفاضل بسته بوده وشامل عضو 1 (در اینجا منظور S است) و عضو 0 (در اینجا منظور $\varnothing$ است) است را یک میدان (مجموعه) می‌نامیم. مجموعه‌ای از پیشامدهای $\mathcal{F}$ همراه با تابع (تابع مجموعه‌ای) وابسته P، که اندازه روی $\mathcal{F}$ نامیده می‌شود، میدان احتمال[۴] نامیده می‌شود و با $(\mathcal{F}, P)$ نمایش می‌دهیم. نشان دادن سازگاری اصول A۱ تا A۶ آسان است. این توسط روش معمول که با ساخت مثالی که اصول را تصدیق می‌کند معلوم شده است. فرض کنید S از یک عنصر تشکیل شده باشد، مجموعه پیشامدها S و پیشامد تهی $\varnothing$ شود و $P(S) = 1$ و $P(\varnothing) = 0$ باشد. بررسی اینکه این سیستم اصول فوق را ارضا می‌کند آسان است. به هر حال، مجموعه اصول ناتمام است: برای مسئله‌های مختلف در نظریه احتمال مجبوریم میدان‌های احتمال مختلف بسازیم.

مثال ۲.۶.۱. P را که از اصول زیر به دست می‌آید توزیع احتمال روی S می‌گوییم. برای هر پیشامد

[۴] Probability Field

E، $0 \leq P(E) \leq 1$؛ $P(\varnothing) = 0$؛ اگر $A \subseteq B$ باشد، آنگاه $P(A) \leq P(B)$؛ اگر $\overline{A}$ متمم $S - A$ از A باشد، آنگاه $P(\overline{A}) = 1 - P(A)$؛ و $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.

۷.۱ پیچیدگی کولموگروف

مفهوم پیچیدگی کولموگروف ریشه در نظریه احتمال، نظریه اطلاع و مفاهیم فلسفیِ «بی‌نظمی» دارد و با استفاده از توسعه‌ی اخیر نظریه الگوریتم‌ها به ثمر نشسته است. این ایده ارتباط نزدیکی به مسائل در هر دو نظریه احتمالات و نظریه اطلاع دارد. این مسائل آنطور که در ادامه مطرح می‌شوند می‌توانند چنین تفسیر شوند که رشته‌های مرتبط به اندازه کافی کامل و دقیق نیستند؛ آن‌ها مسائلی را مشخص نشده باقی می‌گذارند که شهودمان می‌گوید باید روی آن‌ها بررسی بیشتری صورت گیرد.

۱.۷.۱ خلاء نظریه احتمال کلاسیک

یک مدعی مخالف بیان می‌کند که یک سکه متعادل راستگو داریم. به هر حال، زمانی که او سکه را صد بار پرتاب می‌کند، سکه صد بار رو می‌آید. به محض مشاهده این موضوع، ادعا می‌کنیم که سکه نمی‌تواند متعادل باشد. مدعی در نظریه احتمال تجدید نظر کرده و می‌گوید هر دنباله از نتایجِ صدبار پرتاب سکه دارای احتمال یکسان $\frac{1}{2^{100}}$ می‌باشد و یک دنباله باید بیاید.

نظریه احتمال هیچ پایه و اساسی برای به چالش کشیدن نتیجه بعد از اتفاق افتادن آن را به ما نمی‌دهد. ما تنها می‌توانیم با استفاده از قرار دادن شرط روی یک نتیجه از صد گزینه به رد غیر منصفانه بودن در اجرا بپردازیم. اما در مورد ...۱۰۱۰ چگونه؟ در مورد یک بخش ابتدایی از بسط دودویی π چگونه؟

دنباله‌ی منظم $Pr(00000000000000000000000000) = \frac{1}{2^{26}}$،

دنباله‌ی منظم $Pr(01000110110000010100111001) = \frac{1}{2^{26}}$ و

دنباله‌ی تصادفی $Pr(10010011011000111011010000) = \frac{1}{2^{26}}$.

دنباله‌ی اولی منظم است، اما فرق دنباله‌ی دوم و سوم در چیست؟ دنباله‌ی سوم توسط به هم زدن

یک چارک تولید شده بود. دنباله دوم خیلی با قاعده است: $0, 1, 00, 01, \ldots$. دنباله سوم آزمون‌های تصادفی (کاذب) را منتقل می‌کند.

در حقیقت نظریه احتمال کلاسیک نمی‌تواند مفهوم تصادفی بودن یک دنباله منحصر به فرد را بیان کند. آن تنها می‌تواند انتظارات مشخصات نتایج پردازش تصادفی را بیان کند، که تحت برخی توزیع‌ها، انتظارات مشخصات مجموعه کامل از دنباله ها است.

فقط در همین اواخر، این مشکل توسط ترکیب مفاهیم محاسبه‌پذیری و آمار برای بیان پیچیدگی اشیاء متناهی حل رضایت‌بخشی پیدا کرده است. این پیچیدگی طول کوتاه‌ترین برنامه دودویی است که آن شیء می‌تواند به طور مؤثر با آن مشخص شود. پیچیدگی یک شیء ممکن است محتوای الگوریتم اطلاعی آن شیء نامیده شود. این کمیت مشخصه یک شیء را به تنهایی تولید می‌کند و پیچیدگی کولموگروف آن شیء نامیده می‌شود.

نظریه اطلاع کلاسیک شانون[۵]، کمیت اطلاع را به یک مجموعه از پیام‌های ممکن اختصاص می‌دهد. همه‌ی پیام‌ها در مجموعه احتمال یکسانی دارند. این کمیت تعداد بیت‌های مورد نیاز برای شمارش تمام احتمالات است و این حقیقت را بیان می‌کند که هر پیام در مجموعه می‌تواند با استفاده از این تعداد بیت‌ها ارتباط برقرار کند. به هر حال، چیزی درباره‌ی تعداد بیت‌های مورد نیاز برای انتقال پیام منحصر به فرد در مجموعه بیان نمی‌کند. برای توضیح این موضوع، مجموعه را شامل تمام رشته‌های دودویی به طول ۹۹۹۹۹۹۹۹۹۹۹۹۹۹۹ در نظر بگیرید. با اندازه‌گیری شانون، ما به طور میانگین به ۹۹۹۹۹۹۹۹۹۹۹۹۹۹۹ بیت برای کدگذاری یک رشته در چنین مجموعه‌ای نیازمندیم. یک شرط برای این کار این است که ما روی یک الگوریتم توافق کنیم که رشته‌های کدگذاری شده را کدگشایی کند. ما می‌توانیم رشته‌ها را با ذکر اینکه ۹۹۹۹۹۹۹۹۹۹۹۹۹۹۹ برابر ۱۱۱۱۱۱۱۱۱۱۱۱۱۱۱ × ۳۲ و ۱۱۱۱۱۱۱۱۱۱۱۱۱۱۱ شامل ۲۴ تا ۱ است، دوباره فشرده‌سازی کنیم.

بنابراین ما به یک پدیده‌ی جالب توجه دست پیدا می‌کنیم: توصیف برخی از رشته‌ها به طور قابل توجهی می‌تواند فشرده شود، به شرط آنکه به اندازه کافی منظم نمایش داده شده باشند. البته این اظهار نظر، اساس و پایه‌ی تمام سیستم‌ها برای بیان اعداد خیلی بزرگ می‌باشد و در اوایل توسط ارشمیدس

[۵] Shannon's Classical Information Theory

در رساله شمارش شن به کار برده شده بود، که در آن رساله، وی یک سیستم برای نام‌گذاری اعداد خیلی بزرگ پیشنهاد داده است. به هر حال، اگر نظم وجود نداشته باشد، مایه زحمت بیشتر برای بیان اعداد بزرگ می‌شود. برای مثال، به نظر می‌رسد فشرده کردن عدد یک میلیارد آسان‌تر از فشرده کردن عدد یک میلیارد و هفتصد و سی و پنج میلیون و دویست و سی و شش هزار و سیصد و نود و چهار باشد، حتی اگر هر دو از نظر مقدار، گستردگی یکسان داشته باشند.

فصل ۲

نظریه‌ی الگوریتمی اطلاع

مفهوم اساسی نظریه الگوریتمی اطلاع، همچنان که شایتین ارایه داده بود، محتوای اطلاع یک شیء خاص است که میزان سختی تعیین، تشریح یا محاسبه‌ی آن شیء می‌باشد. هدف اصلی آن، تلاش برای اعمال نظریه‌ی اطلاعی و ایده‌های احتمالی در نظریه‌ی توابع بازگشتی و فراریاضیات است. بخصوص، این نظریه قادر است قضیه‌ی ناتمامیت اول گودل را با تعریف درجه‌های ناتمامیت سیستم‌های صوری تصحیح کرده و در محتوای الگوریتمی اطلاع این نظریه‌ها شرح دهد ([۴، ۵، ۶، ۷، ۸، ۹]). دیدگاه‌های شایتین از معروفیت مسلمی برخوردار شد، گواه این مطلب، آورده شدن دو مقاله‌ی وی در مجموعه‌ی «راهبردهای نوین در فلسفه‌ی ریاضیات» در سال ۱۹۸۶ می‌باشد [۴۰]. در این فصل نشان می‌دهیم که ریاضیات شایتین نتایج فلسفیش را تایید نمی‌کند. ما دو کاربرد از نظریه الگوریتمی اطلاع را مورد مطالعه قرار می‌دهیم: در بخش ۱.۲، تفسیر مطرح قضیه‌ی اول ناتمامیت را به عنوان یک قضیه در مورد محتوای اطلاع مورد بحث قرار می‌دهیم [۴]، [۶] و [۷]، و در بخش ۲.۲، در مورد دلیل کشف «تصادفی بودن در ریاضیات» بحث خواهیم کرد [۸] و [۹].

۱.۲ محدودیت‌های نظریه-اطلاعی سیستم‌های صوری

ادعای شایتین مبنی بر اینکه نظریه الگوریتمی اطلاع زمینه‌ی مناسبی برای بحث قضیه‌ی اول ناتمامیت گودل آماده می‌کند، شامل دو قسمت است:

(الف) نشان دادن اینکه برای هر سیستم صوری صحیح $\mathbf{T}$ شامل حساب، می‌توان ثابت $c_{\mathbf{T}} \in \mathbb{N}$ را نسبت داد به طوری که $\mathbf{T}$ نمی‌تواند حکم «$K(w) > c_{\mathbf{T}}$» را ثابت کند که در آن w یک رشته‌ی دودویی متناهی دلخواه و $K(w)$ پیچیدگی کولموگروف w است. شایتین بیان می‌کند که ارتباط کمی دقیقی بین $c_{\mathbf{T}}$ و «محتوای اطلاع» یا «بی‌نظمی» سیستم صوری $\mathbf{T}$ وجود دارد:

> در اینجا قضیه‌ی ناتمامیت برای نظریه اصل موضوعی صوری است که نتایج حسابی آن‌ها درست است. مجموعه‌ی فوق به صورت زیر است: اصول، یک رشته‌ی متناهی است و قواعد استنتاج، الگوریتمی برای شمارش قضایای اصول داده شده هستند. مطابق با چنین سیستم صوری، یک رشته‌ی خاص که بی‌نظمی (پیچیدگی) آن بزرگتر از بی‌نظمی اصول نظریه است نمی‌تواند اثبات شود. متقابلاً، سیستم‌های صوری وجود

دارند که اصول آن‌ها دارای بی‌نظمی $n + O(1)$ هستند به طوری که ممکن است تمام گزاره‌های درست به شکل «$K(\text{رشته‌ی خاص}) > n$» را ایجاد کنند [۶].

(ب) هدف نهایی شایتین حتی بیشتر جاه‌طلبانه بود:

برهان اصلی گودل یک حکم مهمل‌نما را ساخته بود که درست است اما مطابق صوری‌سازی معمول نظریه اعداد قابل اثبات نیست. در مقابل، من می‌خواهم قدرت مجموعه‌ای از اصول و قواعد استنتاج را اندازه‌گیری کنم. می‌خواهم قادر به بیان این مطلب باشم که اگر کسی ده کیلو اصل و بیست کیلو قضیه داشته باشد، آنگاه قضیه نمی‌تواند از اصول استنتاج شود. [...] برای مشخص‌تر شدن، دیدگاه ترمودینامیکی و مکانیک آماری را برای قضیه‌ی گودل اعمال نموده و از چنین مفهومی برای احتمال، تصادفی بودن، بی‌نظمی و پیچیدگی اطلاع استفاده خواهم کرد تا پدیده‌ی ناتمامیت را مطالعه کرده و تلاش می‌کنم چگونگی گسترش آن را تعیین کنم [۷].

اگرچه قضیه‌ی اشاره شده برای عبارت اولی معتبر است، اما تاکید روی «بی‌نظمی اصول نظریه» کمی گمراه کننده به نظر می‌رسد. در حقیقت، با استفاده از یک کاربرد ساده از قضیه‌ی بازتابی ارایه شده توسط کریزل[۱] و لوی[۲]، نشان داده می‌شود که یک گردایه نامتناهی C از نظریه‌های حسابی متفاوت $\mathbf{T}$ وجود دارد به طوری که هیچ رابطه‌ی جالب توجهی بین $\mathbf{T}$ و کوچکترین $c_{\mathbf{T}}$ها که برای همه‌ی wها، $\mathbf{T} \nvdash K(w) > c_{\mathbf{T}}$، موجود نیست. با صراحت بیشتر، از آنجایی که با استفاده از خواص پیچیدگی کولموگروف، حتی بی‌نظمی روی C محدود نیست، تمام $\mathbf{T}$ها در C همان کوچکترین $c_{\mathbf{T}}$ را دارند به طوری که برای تمام wها، $\mathbf{T} \nvdash K(w) > c_{\mathbf{T}}$. چنین به نظر می‌رسد که محتوای نظریه اطلاع (همچنان که به عنوان پیچیدگی کولموگروف اصول تعریف شده بود) فقط مربوط به حاشیه‌ی پدیده‌ی ناتمامیت ذکر شده در (الف) است، و بنابراین توقع بیان شده در (ب) کمی نابهنگام به نظر می‌رسد. به علاوه، مشاهده خواهد شد که تنها با استفاده از موضوع گیج کننده‌ی زبان و فرازبان

[۱] Kreisel

[۲] Levy

می‌توان گفت که (الف) قسمت (ب) را نتیجه می‌دهد. نتیجه‌ی کلی این است که ساختار شایتین تاکنون تعریفی از قضیه اول ناتمامیت ارایه نکرده است.

۱.۱.۲ پیچیدگی کولموگروف

اگرچه شایتین [۵، ۶، ۷، ۸، ۹] یک مفهوم کمی متفاوت از پیچیدگی را استفاده کرده است، اما ضروریات می‌توانند با مفهوم ساده‌تر توضیح داده شوند.

تعریف ۱.۱.۲. فرض کنید که $A : 2^{<\omega} \to 2^{<\omega}$ یک تابع بازگشتی جزیی با عدد گودل[۱] $\ulcorner A \urcorner$ باشد. اگر w یک رشته‌ی دودویی متناهی باشد، آنگاه $l(w)$ طول w را نشان می‌دهد. پیچیدگی w نسبت به A را که با $K_A(w)$ نشان می‌دهیم، به صورت زیر تعریف می‌شود:

$$K_A(w) = \begin{cases} \infty & \text{اگر هیچ } p \text{ای موجود نباشد که } A(p) = w \\ l(p) & \text{اگر } p \text{ کوتاه‌ترین ورودی باشد که } A(p) = w \end{cases} . \qquad (۱.۲)$$

یک ماشین تورینگ جهانی Φ مجانباً بهینه نامیده می‌شود هرگاه توسط مقتضیاتی تعیین شده باشد که روی ورودی به شکل $q = 0^{\ulcorner A \urcorner}1p$، Φ همان عمل A روی p را اعمال کند. عددگذاری گودل و یک ماشین جهانی مجانباً بهینه Φ را در نظر بگیرید و قرار دهید $K(w) := K_\Phi(w)$. K پیچیدگی کولموگروف w نامیده می‌شود [۱۸، ۱۹، ۲۰، ۲۱، ۲۲]. ورودی‌ها همواره برنامه نامیده خواهند شد.

دیدیم که هر عدد طبیعی با نمایش دودویی آن شناخته می‌شود، این نمایش مفهومی برای بحث پیچیدگی یک عدد طبیعی ایجاد می‌کند. به وضوح لم زیر را داریم:

لم ۲.۱.۲. *(الف) برای هر تابع بازگشتی جزیی $A : 2^{<\omega} \to 2^{<\omega}$ و تمام wها،*

$$K(w) \leq K_A(w) + \ulcorner A \urcorner + 1 .$$

[۱] برای تعریف عدد گودل، فصل ۱۵ مرجع [۲] را مطالعه کنید.

(ب) *برای بعضی ثوابت c و تمام wها*، $K(w) \leq l(w) + c$ [۲۷].

یک شمارش ساده نشان خواهد داد که برای هر m، بی‌نهایت دنباله‌ی w با خاصیت $K(w) > m$ وجود دارد. درنتیجه، عبارت «$\#A$» برای تعداد عناصر مجموعه‌ی (متناهی) A توقف می‌کند و 2^n نشان دهنده‌ی مجموعه‌ی رشته‌های دودویی از طول n است.

لم ۲.۱.۳. (*الف*) $\#\{w \in 2^n | K(w) \leq n - m\} \leq 2^{(n-m+1)} - 1$.

(ب) $\#\{w \in 2^n | K(w) > n - m\} > 2^n \cdot (1 - 2^{-m+1})$.

(پ) m *را ثابت در نظر بگیرید، در این صورت برای تمام nهای به اندازه کافی بزرگ $w \in 2^n$ وجود دارد به طوری که* $K(w) > n - m$.

برهان. (الف) تعداد برنامه‌های روی Φ که طول کمتر از $n - m$ دارند، کمتر از $2^{n-m+1} - 1$ است. بنابراین (ب) حداقل $2^n - 2^{n-m+1} = 2^n \cdot (1 - 2^{-m+1})$ دنباله در 2^n، $K(w) > n - m$ را ارضا می‌کنند. قسمت (پ) نیز بلافاصله از (ب) نتیجه می‌شود. □

به سادگی بیش از حد برهان توجه کنید: این استدلال در هر سیستم مبتنی بر منطق کلاسیکی که بتواند مجموعه‌های متناهی از اعداد صحیح را بررسی کند می‌تواند صوری‌سازی شود. این مغایر با حقیقت اثبات شده در نتیجه‌ی ۷.۱.۲، که مجموعه‌ی $\{w | K(w) > g(l(w))\}$ که در آن g یک تابع بازگشتی تام صعودی بوده است: گرچه مجموعه‌ی فوق نامتناهی است، اما شامل هیچ زیر مجموعه‌ی شمارای کارآمد نیست.

۲.۱.۲ ناتمامیت نظریه-اطلاعی

در این بخش ثابت می‌شود که برای هر سیستم صوری صحیح $\mathbf{T}$ ثابت $c_{\mathbf{T}}$ چنان موجود است که برای تمام رشته‌های دودویی متناهی w، $\mathbf{T} \nvdash K(w) > c_{\mathbf{T}}$. به چندین دلیل که در ادامه توضیح خواهیم داد، ما دو برهان ارایه می‌دهیم که هر دو با برهان شایتین متفاوت است. ما از نمادگذاری راجرز[۲] برای توابع بازگشتی جزیی و مجموعه‌های شمارای کارآمد استفاده می‌کنیم [۳۲]: ϕ_n تابع

[۲] Rogers

بازگشتی جزیی از $\mathbb{N}$ به $\mathbb{N}$ با عدد گودل n و W_e زیرمجموعه‌ی شمارای کارآمد از $\mathbb{N}$ با عدد گودل e را نمایش می‌دهند. طبق معمول، باید فرض کنیم که مجموعه‌ها، همانند $2^{<\omega}$ یا $\omega \times 2^{<\omega}$ و غیره، با اعداد طبیعی کد شده‌اند.

لم ۴.۱.۲. *مجموعه‌ی* $\{\langle w, m\rangle \in 2^{<\omega} \times \omega | K(w) \leq m\}$[1] *شمارای کارآمد است.*

برهان. اگر Φ همان ماشین تورینگ جهانی تعریف شده در ۱.۱.۲ باشد، با استفاده از تعریف K خواهیم داشت:

$$\{\langle w, m\rangle \in 2^{<\omega} \times \omega | K(w) \leq m\} = \{\langle w, m\rangle \in 2^{<\omega} \times \omega | \exists p(\Phi(p) = w \ \& \ l(p) \leq m)\}$$؛

شرط سمت راست Σ_1 است. □

بنابراین مجموعه‌ی $\{\langle w, m\rangle \in 2^{<\omega} \times \omega | K(w) > m\}$، Π_1 است؛ اما یک خاصیت قوی‌تری را نیز ارضا می‌کند.

تعریف ۵.۱.۲. (الف) مجموعه‌ی A مصون گفته می‌شود هرگاه نامتناهی بوده و شامل هیچ زیرمجموعه‌ی شمارای کارآمد نامتناهی نباشد.

(ب) مجموعه‌ی A به طور کارآمد مصون گفته می‌شود هرگاه برای یک تابع بازگشتی تام مانند $g : \omega \to \omega$، $W_e \subseteq A$ ایجاب کند که $\#W_e \leq g(e)$.

(پ) مجموعه‌ی B (به طور کارآمد) ساده گفته می‌شود هرگاه شمارای کارآمد بوده و B^C (به طور کارآمد) مصون باشد.

قضیه ۶.۱.۲. *ثابت* d *چنان موجود است که هر زیرمجموعه‌ی شمارای کارآمد* W_e *از مجموعه‌ی* $\{\langle w, m\rangle \in 2^{<\omega} \times \omega | K(w) > m\}$ *در مختص دوم توسط* $K(e) + d$ *کراندار است.*

برهان. اگرچه نتیجه فقط برای K بیان شده، اما طیف گسترده‌ای از معیارهای پیچیدگی را دربر می‌گیرد. بدین سبب، برهان مختصری ارایه می‌دهیم. Φ را الگوریتم جهانی در نظر گرفته و یک تابع بازگشتی جزیی f را به شکل زیر تعریف می‌کنیم: f روی ورودی‌های به شکل $0^n 1 q$ عمل می‌کند.

[1] $2^{<\omega}$ نشان دهنده‌ی مجموعه‌ی تمام دنباله‌های متناهی متشکل از 0 و 1 است.

با توجه به این ورودی، ابتدا f مقدار $\Phi(q)$ را محاسبه می‌کند، اگر و فقط اگر زمانی که $e = \Phi(q)$ را یافت، W_e را تا زمانی تولید کند که $\langle w, m\rangle \in W_e$ را پیدا کرده باشد به طوری که $m > l(q)+n+1$؛ آنگاه خروجی w را بدهد. حال فرض کنید که $W_e \subseteq \{\langle w, m\rangle \in 2^{<\omega} \times \omega | K(w) > m\}$. قضیه‌ی بازگشت را برای به دست آوردن nای که برای تمام qها، $\phi_n \simeq f(0^n 1q)$، اعمال می‌کنیم. q_0 را همان عددی در نظر بگیرید که $e = \Phi(q_0)$. ادعا می‌کنیم که $\phi_n(q_0)$ تعریف نشده است. فرض (خلف) کنید که $\phi_n(q_0) = w$. آنگاه از یک طرف، با توجه به ساختار،

$$K(w) > m > l(q_0) + n + 1;$$

از طرف دیگر، با توجه به لم ۲.۱.۲،

$$K(w) \leq K_{\phi_n}(w) + n + 1 \leq l(q_0) + n + 1.$$

بنابراین $\phi_n(q_0)$ تعریف نشده است. این نشان می‌دهد که $K(e) + n + 1$ کران بالایی برای مختص دوم W_e می‌باشد. □

ابتدا قضیه‌ای را برای به دست آوردن برخی اطلاعات نظریه بازگشتی روی K اثبات می‌کنیم.

نتیجه ۷.۱.۲. *فرض کنید که $g : \omega \to \omega$ تابع بازگشتی تام بوده، $\lim_{n\to\infty} g(n) = \infty$ و برای یک m طبیعی $\forall n : g(n) \leq n - m$. آنگاه مجموعه‌ی $\{w | K(w) > g(l(w))\}$ مصون است. به علاوه، اگر به طور بازگشتی داشته باشیم $\lim_{n\to\infty} g(n) = \infty$، آنگاه مجموعه‌ی $\{w | K(w) > g(l(w))\}$ شمارای کارآمد است.*

برهان. فرض کنید $W_e \subseteq \{w | K(w) > g(l(w))\}$. قرار دهید $V_e := \{\langle w, g(l(w))\rangle | w \in W_e\}$؛ در این صورت برای یک تابع بازگشتی تام f، داریم $V_e = W_{f(e)}$. چون $W_{f(e)} \subseteq \{\langle w, m\rangle | K(w) > m\}$، درنتیجه $W_{f(e)}$ در مختص دومش کراندار است. به عنوان مثال، توسط $\log_2 f(e)$. اما از آنجایی که $\lim_{n\to\infty} g(n) = \infty$ پس W_e می‌بایستی متناهی باشد و اگر به طور بازگشتی داشته باشیم $\lim_{n\to\infty} g(n) = \infty$، آنگاه می‌توانیم به طور کارآمد $n_0(e)$ را چنان انتخاب کنیم که برای $n \geq n_0(e)$، $\log_2 f(e) \leq g(n)$. بنابراین درنهایت خواهیم داشت $\#W_e \leq 2^{n_0(e)+1}$. □

این نتیجه این طور ادامه می‌یابد که مجموعه‌ی شمارای کارآمد $\{\langle w,m\rangle|K(w)\leq m\}$ بازگشتی نبوده و به علاوه تابع $K:2^{<\omega}\to\omega$ بازگشتی نیست.

مثال ۲.۱.۸. مجموعه‌ی رشته‌های تصادفی $\{w|K(w)>l(w)-m\}$ به طور کارآمد مصون است. طبق قضیه‌ای از مارتین[۲] [۳۸]، مجموعه‌ی $\{w|K(w)\leq l(w)-m\}$ یک مجموعه‌ی شمارای کارآمد کامل است.

حال نیمه‌ی اول قضیه‌ی ناتمامیت شایتین را فرمول‌بندی می‌کنیم. برای هر عدد طبیعی m، تمام wها (به جز تعداد محدودی) $K(w)>m$ را ارضا می‌کنند. ما این را در بخش ۱.۱.۲ اثبات کردیم. اثبات تنها با استفاده از خواص ابتدایی مجموعه‌های متناهی، می‌تواند در هر نظریه‌ی (کلاسیک) که شامل قسمت کوچکی از حساب باشد، فرمول‌بندی شود. با این حال، همچنان که قضیه‌های زیر نشان می‌دهند، تقریباً تحقیق در مورد بعضی رشته‌های خاص با پیچیدگی کولموگروف بزرگ غیرممکن است.

قضیه ۲.۱.۹. *فرض کنید $\mathbf{T}$ یک سیستم صوری صحیح باشد که با مجموعه‌ی قضیه‌های شمارای کارآمدش شناخته می‌شود. p را یک اندیس شمارای کارآمد برای $\mathbf{T}$ در نظر بگیرید. در این صورت، برای برخی از ثوابت d، مستقل از $\mathbf{T}$، و برای تمام wها $\mathbf{T}\nvdash K(w)>K(p)+d$.*

برهان. تمام قضیه‌هایی از $\mathbf{T}$ را که به شکل $K(w)>m$ نیستند، حذف کرده و نتیجه را سیستم صوری صحیح $\mathbf{T}'$ می‌نامیم. این عملکرد بازگشتی ابتدایی است. $\mathbf{T}'$ ممکن است با زیرمجموعه‌ی شمارای کارآمد از $\{\langle w,m\rangle\in 2^{<\omega}\times\omega|K(w)>m\}$ با عدد گودل p' شناخته شود. با استفاده از قضیه ۲.۱.۶، $\mathbf{T}'$، برای بعضی از ثوابت d' که به p' وابسته نیست، توسط $K(p')+d'$ در مختص دومش کراندار است. اما برای بعضی cها، $K(p')\leq K(p)+c$. □

ملاحظه ۲.۱.۱۰. *چون عملکردی که ما را از $\mathbf{T}$ به $\mathbf{T}'$ می‌رساند بازگشتی ابتدایی است، البته درست است که برای بعضی dها $\mathbf{T}$ هیچ عبارتی به شکل «$K(w)>K(p)+d$» را ثابت نمی‌کند که در آن p یک اندیس شمارای کارآمد برای $\mathbf{T}$ است، اما پیش از این، جریان فوق اشاره‌ای به این مطلب*

[۲] Martin

دارد که $K(p)$ ، محتوای اطلاع سیستم صوری $\mathbf{T}$ ، ممکن است ارتباطی به تعیین کوچک‌ترین cای که برای تمام wها $\mathbf{T} \nvdash K(w) > c$ ، نداشته باشد. اجازه دهید کوچک‌ترین چنین cها را که به $\mathbf{T}$ وابسته است ثابت مشخصه ی سیستم صوری $\mathbf{T}$ نامیده و از این به بعد با $c_{\mathbf{T}}$ نشان دهیم. پس برهان فوق احتمال اینکه در بسیاری از موارد نظریه‌های متفاوت، به عنوان مثال **PA** *یا* **ZF** *، همان ثابت مشخصه را داشته باشند، باز گذاشته است. در ادامه وضعیت درستی وقوع چنین اتفاقی را خواهیم دید.*

حال روشی کاملا متفاوت از تعیین ثابت c را ارایه می‌دهیم به طوری که (برای مثال) **PA** هیچ عبارتی به شکل «$K(w) > c$» را ثابت نمی‌کند. این دیدگاه از ویسِر[۳] و یانگ[۴] منشاء گرفته است.

قضیه ۱۱.۱.۲. *ثابت c چنان موجود است که* **PA** *هیچ عبارتی به شکل «$K(w) > c$» را ثابت نمی‌کند.*

برهان. فهرستی از برهان‌های **PA** را در نظر بگیرید و تابع بازگشتی جزیی ϕ_e را به صورت زیر تعریف کنید: $\phi_e(m) = n$ اگر و تنها اگر n، برابر kای در اولین برهان عبارتی به شکل «$\phi_m(m) \neq k$» در **PA** باشد. ادعا می‌کنیم که $\phi_e(e)$ تعریف نشده است. فرض(خلف) می‌کنیم که $\phi_e(e) = n$ باشد، در این صورت $\mathbf{PA} \vdash \phi_e(e) \neq n$ که یک تناقض است. این نتیجه می‌دهد که $\mathbf{PA} + \{\phi_e(e) = n\}$ برای هر n سازگار است، زیرا اگر $\mathbf{PA} \vdash \phi_e(e) \neq n$ بنابراین $\phi_e(e)$ تعریف خواهد شد. چون برای تمام nها، $\mathbf{PA} + \{\phi_e(e) = n\}$ سازگار است، $\mathbf{PA} + \{K(n) \leq 2e + 1\}$ نیز سازگار می‌باشد. بنابراین، **PA** هیچ عبارتی به شکل «$K(n) > 2e + 1$» را ثابت نمی‌کند. □

البته این برهان برای سیستم‌های صوری دیگر نیز اعمال می‌شود. استدلال بالا به طور متقاعدکننده‌ای نشان می‌دهد که هیچ دلیل مستدلی برای توقع اینکه $c_{\mathbf{T}}$ و محتوای اطلاع $\mathbf{T}$ (همچنان که به عنوان پیچیدگی کولموگروف اصولش تعریف شده) مرتبط باشند وجود ندارد.

ملاحظه ۱۲.۱.۲. *در نقل قول شایتین که در ابتدای این فصل آوردیم، همواره همخوانی ضعیفی با قضیه‌ی ۲ .۱ .۹ که «سیستم‌های صوری وجود دارند که اصول آن‌ها دارای بی‌نظمی $n + O(1)$ هستند*

[۳] Visser

[۴] Jongh

به طوری که ممکن است تمام گزاره‌های درست به شکل «$n <$ (رشته‌ی خاص)K» را استدلال کنند.» وجود دارد. برای اهدافمان لازم نیست این نتیجه را اثبات کنیم. فقط ملاحظه می‌کنیم که همخوانی کامل با قضیه‌ی ۲ .۱ .۹ اینگونه خوانده خواهد شد: «تمام نظریه‌های صوری که اصول آن‌ها دارای بی‌نظمی $n + O(1)$ باشند، تمام گزاره‌های درست به شکل «$n <$ (رشته‌ی خاص)K» را استدلال می‌کنند.» اما استدلالی که در ادامه می‌آید نشان می‌دهد که این عبارت نادرست است.

۳.۱.۲ استفاده از قضیه‌ی بازگشت

ملاحظه ۱۳.۱.۲. اگرچه قضیه‌ی ۲ .۱ .۹ به عنوان یک «توسیع عظیمی از قضیه گودل» نامیده شده بود [۱۱]، ما نباید فراموش کنیم که تفاوت بزرگی بین دو نتیجه وجود دارد. قضیه‌ی اول ناتمامیت گودل ساختار صریحی از یک Π_1- فرمول (درست و) تصمیم‌ناپذیر ارایه می‌دهد: موضوع لم ۲ .۱ .۱۶ ، در یک روش بازگشتی ابتدایی، هر سیستم صوری $\mathbf{T}$ را به یک فرمول $\psi_{\mathbf{T}}$ که بیان می‌کند «در $\mathbf{T}$ غیرقابل اثبات هستم» مربوط می‌کند. اما نه قضیه‌ی ۲ .۱ .۹ و نه ۲ .۱ .۱۱ تفسیر صریحی فراهم نمی‌آورند. برای مثال به قضیه‌ی ۲ .۱ .۹ توجه کنید، اولا ، برهانش نشان می‌دهد که محتوای اطلاع سیستم صوری $\mathbf{T}$ یک تابع بازگشتی از $\mathbf{T}$ نیست. دوما، فرض کنید که کران بالای بازگشتی $f(\mathbf{T})$ را برای محتوای اطلاع $\mathbf{T}$ داشته باشیم، در این صورت هنوز تعیین بازگشتی کلمه‌ی $w(\mathbf{T})$ به طوری که $K(w(\mathbf{T})) > f(\mathbf{T}) \geq c_{\mathbf{T}}$ غیرممکن است. اگر این چنین می‌بود، می‌توانستیم یک دنباله شمارای کارآمد متناهی از سیستم صوری $\mathbf{T}_n$ و کلمه‌ی $w_{\mathbf{T}_n}$ را که $K(w(\mathbf{T}_n)) > f(\mathbf{T}_n)$ و $f(\mathbf{T}_n) \to \infty$ به صورت زیر تعریف کنیم: $\mathbf{T}_0 = \mathbf{PA}$ ، $\mathbf{T}_1 = \mathbf{T}_0 \cup \{K(w(\mathbf{T}_0)) > f(\mathbf{T}_0)\}$ و الی آخر. با توجه به ساختار، $c_{\mathbf{T}_n} < c_{\mathbf{T}_{n+1}}$ و بنابراین داریم $\lim_{n\to\infty} f(\mathbf{T}_n) = \infty$. اما نتیجه ۲ .۱ .۷ بیان می‌کند که تنها تعداد متناهی $w(\mathbf{T}_n)$ را می‌توان ساخت. بنابراین تعیین کارآمد یک سیستم صوری $\mathbf{T}$ و کلمه‌ی $w(\mathbf{T})$ داده شده که برای آن‌ها $K(w(\mathbf{T})) > c_{\mathbf{T}}$ باشد، غیرممکن است. در این مضمون، قضیه‌ی ۲ .۱ .۹ شکل ضعیفی (به جای یک تعمیم) از قضیه‌ی اول ناتمامیت است. یک استدلال مشابه برای قضیه‌ی ۲ .۱ .۱۱ اعمال می‌شود.

ملاحظه ۱۴.۱.۲. حال نشان می‌دهیم که $c_{\mathbf{T}}$ به طور کلی قرابتی با محتوای اطلاع سیستم صوری

$\mathbf{T}$ ندارد، که مقصودمان از «قرابت» تفاوت محدود بین دو کمیت است. با استفاده از قضیه‌ی ۱۱ کریزل و لوی [۲۳]، قطعه‌های حسابی $\mathbf{ZF}$ به طور متناهی روی $\mathbf{PA}$ اصل‌پذیر نیستند. قضیه‌ی ۲ .۱ .۹ ثوابت $c_{\mathbf{PA}}$ و $c_{\mathbf{ZF}}$ را اختصاص می‌دهد به طوری که هیچ عبارتی به شکل «$K(w) > c_{\mathbf{PA}}$» و «$K(w) > c_{\mathbf{ZF}}$» به ترتیب در $\mathbf{PA}$ و $\mathbf{ZF}$ اثبات‌پذیر نیستند. تعداد نامتناهی از نظریه‌های (عددی قوی) $\mathbf{T}_n$ که در بین $\mathbf{PA}$ و (یک قطعه‌ی حسابی از) $\mathbf{ZF}$ قرار دارد می‌بایست همان ثابت مشخصه‌ی c را داشته باشند و همان مجموعه از عبارات به شکل «$K(w) > m$» را ثابت کنند. چون K روی اصول $\mathbf{T}_n$ بی‌کران است، ثابت مشخصه‌ی $\mathbf{T}_n$ قرابتی با محتوای اطلاع این اصول ندارد. به عبارت دیگر، در واقع محتوای اطلاع اصول، «محدودیت‌های بیرونی ممکن» را فراهم می‌کنند [۹]، و محدودیت‌های واقعی را باید جای دیگر جستجو کرد.

ملاحظه ۱۵.۱.۲. *به علاوه، چیز خاصی در قضیه‌ی ۲ .۱ .۹ وجود ندارد که ادعای شایتین را تایید کند (در قسمت (ب) در ابتدای این فصل توضیح داده شد) که تصمیم‌ناپذیری یک فرمول می‌تواند به عنوان نتیجه‌ای از یک محتوای اطلاع اضافی توضیح داده شود. مشاهده می‌شود که چیز خاصی درباره‌ی محتوای اطلاع فرمول «$K(w) > c_{\mathbf{T}}$» نمی‌گوییم؛ چیزی که اهمیت دارد این است که فرمول تصمیم‌ناپذیر اظهار می‌کند که همان رشته‌ی خاص شامل اطلاعات زیادی است، که بحثی کاملا متفاوت می‌باشد.*

سابقاً این آشفتگی بین زبان اشیا و فرازبان دیده شده بود، اما ساختن عبارت‌های درست که در $\mathbf{PA}$ تصمیم‌ناپذیرند تقریباً توسط قطری‌سازی میسر است، زیرا اگر شرط کنیم که محتوای اطلاع یک عبارت پیچیدگی عدد گودل آن عبارت باشد، اطلاعات خیلی زیادی را شامل می‌شوند. چنین عبارتی با بهره‌گیری از لم نقطه‌ی ثابت ساخته می‌شود:

لم ۱۶.۱.۲. *فرض کنید که ϕ یک فرمول حسابی و در یک متغیر آزاد باشد. در این صورت برای تعداد زیادی ψ، $\mathbf{PA} \vdash \psi \leftrightarrow \phi(\ulcorner\psi\urcorner)$ [۳۶].*

از لم نقطه ثابت برای تعریف جمله‌ی ψ که بیان می‌کنید «حاوی اطلاعات خیلی زیادی از $\mathbf{PA}$ می‌باشم» استفاده می‌کنیم. قرار دهید $k_0 := \max\{m|K(m) \leq c_{\mathbf{PA}}\}$. ψای را (به طور ناکارآمد) انتخاب می‌کنیم که $\ulcorner\psi\urcorner > k_0$ و $\mathbf{PA} \vdash \psi \leftrightarrow [K(\ulcorner\psi\urcorner) > c_{\mathbf{PA}}]$. در اینصورت، $\mathbf{PA} \nvdash \psi$، زیرا در

غیر اینصورت $\mathbf{PA} \vdash K(\ulcorner\psi\urcorner) > c_{\mathbf{PA}}$ که با توجه به قضیه‌ی ۹.۱.۲ غیرممکن است؛ اما ψ درست است زیرا اگر $\neg\psi$ درست می‌بود آنگاه $K(\ulcorner\psi\urcorner) \leq c_{\mathbf{PA}}$ که این نیز ایجاب می‌کند $\ulcorner\psi\urcorner \leq k_0$. چون $\mathbf{PA}$ صحیح است، $\mathbf{PA} \nvdash \neg\psi$. بنابراین ψ درست و تصمیم‌ناپذیر در $\mathbf{PA}$ است. به هر حال، نظر به این که اساساً از این حقیقت استفاده می‌کنیم که نقطات ثابت «$K(\ulcorner\psi\urcorner) > c_{\mathbf{PA}}$» با عدد گودل به اندازه‌ی دلخواه بزرگ وجود دارد، ساختار جزیی است (از اینرو این استدلال برای نشان دادن اینکه $K(\ulcorner\phi\urcorner)$ معیار خوبی از محتوای اطلاع در ϕ نیست، مورد استفاده قرار می‌گیرد). به علاوه، چون هیچ تعیین کارآمدی از $c_{\mathbf{PA}}$ وجود ندارد، نقطه‌ی ثابت بیان نمی‌کند که «حاوی اطلاعات خیلی زیادی از $\mathbf{PA}$ می‌باشم». ملاحظات فوق به طور کامل امکان مفید بودن همان نوع از مفهوم اطلاع در مطالعه‌ی ناتمامیت را رد می‌کنند. آن‌ها نشان می‌دهند که پیچیدگی اصول، معیار خوبی از اطلاعات نیست. به علاوه، اگر اطلاع یک تابع صحیح باشد و از مواردی نظیر قضیه ۹.۱.۲ پیروی کند، آنگاه می‌بایست این نتیجه را قبول کنیم که یک نظریه‌ی $\mathbf{T}_1$ ممکن است قوی‌تر از نظریه‌ی $\mathbf{T}_2$ باشد، در حالی که همان محتوای اطلاع را مانند $\mathbf{T}_2$ داشته باشد. تصور مفهومی از اطلاع که این احتمال را می‌پذیرد سخت است. حتی اگر تولید مفهوم اطلاع برای مطالعه‌ی سیستم‌های صوری مفید باشد، ممکن است ارزش تحقیق درباره‌ی این که چرا خواصِ دیگرِ سیستم‌های صوری به مقدار ثوابت مشخصه‌شان وابسته هستند را نداشته باشد. به هر حال، این تحقیق با کمبود شدید مثال‌های مفهومی متوقف شده بود: همانطور که در بالا اشاره شد، کاری برای دانستن اینکه آیا $c_{\mathbf{PA}} < c_{\mathbf{ZF}}$ انجام نمی‌دهیم، و حتی هیچ ایده‌ای مبنی بر تصدیق نتایجی از این نوع را نداریم.

۲.۲ قضایای ناتمامیت برای اعداد حقیقی تصادفی

شایتین در [۸] و [۹] تلاش می‌کند با نشان دادن اینکه ریاضیات تنها توسط ناتمامیت احاطه نشده است و همچنین با استفاده از تصادفی بودن، تا حدی «شکل نهایی» از قضیه اول ناتمامیت را به معرض نمایش بگذارد. برای بیان ایده‌ی شایتین، ابتدا باید توضیح کوتاهی روی تفاسیر ابتدایی وی بیان کنیم. در [۵]، احتمال توقف Ω از یک ماشین تورینگ جهانی تعریف شده است. این مفهوم تنها می‌تواند برای پیش‌الگوریتم تعریف شود، یعنی الگوریتم‌های A که عبارت «مجموعه‌ی

$\{A(p)$متوقف می‌شود$|p\}$ پیشوند آزاد[۱] است» را ارضا می‌کند. فرض کنید که Φ یک پیش‌الگوریتم جهانی باشد. در این صورت $\{\Phi(p)$متوقف می‌شود$|2^{-l(p)}\}\Sigma =: \Omega$ خوشتعریف است. او سپس یک معادله‌ی سیاله‌ی نمایی $\mathcal{Q} = \mathcal{Q}'$ با خاصیت زیر ایجاد می‌کند:

> $\mathcal{Q} = \mathcal{Q}'$ راه حل‌های متناهی یا نامتناهی دارد. $\mathcal{Q} = \mathcal{Q}'$ کاملاً یک معادله‌ی قابل توجه است، همچنان که نشان می‌دهد نوعی از اصل عدم قطعیت در ریاضیات محض وجود دارد، در حقیقت، حتی در نظریه‌ی تمام اعداد وجود دارد. [...] ممکن است درستی یا نادرستی این ادعا را که تعداد نامتناهی راه حل وجود دارد که غیرقابل تشخیص از نتیجه‌ی مستقل از پرتاب یک سکه‌ی متعادل است [۹].

ادعای قبلی به دلیل این حقیقت است که Ω تعریف تصادفی ارایه شده توسط مارتین-لوف[۲] [۳۰] را ارضا می‌کند. اهمیت فلسفی تفسیر در نتیجه‌گیری [۹] تاکید شده است:

> ... ملاحظه می‌کنیم اثبات اینکه آیا معادلات سیاله‌ی نمایی خاص تعداد متناهی یا تعداد نامتناهی راه حل دارند، مطلقاً لجوجانه است. این قبیل سوالات فراتر از قدرت استدلال ریاضی است. این منطقه که در آن درستی ریاضیات هیچ ساختار قابل تشخیص یا الگویی ندارد، به نظر می‌رسد کاملاً تصادفی است. این سوالات فراتر از قدرت استدلال انسان است. ریاضیات نمی‌تواند به آن‌ها رسیدگی کند. دینامیک غیرخطی و مکانیک کوانتومی نشان داده‌اند که تصادفی بودن در طبیعت وجود دارد. معتقدم که ما در این کتاب دلایلی داریم که تصادفی بودن در حال حاضر در ریاضیات محض است، و در حقیقت، حتی در شاخه‌های نسبتاً ابتدایی نظریه‌ی اعداد است [۹].

۱.۲.۲ تصادفی بودن مارتین-لوف و Δ_2-تعریف‌پذیری

ما به سرعت آن دسته از خواص تعریف مارتین-لوف از تصادفی بودن را بازنگری می‌کنیم که برای اهدافمان نیازمند آن‌ها هستیم. یک شرح کامل می‌تواند در [۳۰] و [۲۶] پیدا شود.

---

[۱] یک مجموعه از کلمه‌های دودویی پیشوند آزاد گفته می‌شود هرگاه هیچ عضوی یک بخش اولیه از عناصر دیگر نباشد.

[۲] Martin-Löf

تعریف ۱.۲.۲. اندازه‌ی احتمال μ روی 2^ω محاسبه‌پذیر نامیده می‌شود هرگاه یک تابع بازگشتی $g : 2^{<\omega} \to \mathbf{Q}$ وجود داشته باشد به طوری که برای تمام w و kها، $|\mu[w] - g(w,k)| < 2^{-k}$، که در آن $[w]$ مجموعه‌ی تمام xهایی است که بخش ابتدایی آن w است.

تعریف ۲.۲.۲. (**مارتین-لوف** [۳۰]). فرض کنید μ یک اندازه‌ی محاسبه‌پذیر باشد. $N \subseteq 2^\omega$ یک آزمون متوالی بازگشتی نسبت به μ است هرگاه N بتواند به عنوان یک Π_2 مجموعه‌ی $\cap_n O_n$ نوشته شده باشد که در آن $O_n \in \Sigma_1$، تابع $n \to O_n$ بازگشتی است، $O_{n+1} \subseteq O_n$ و $\mu(O_n) \leq 2^{-n}$.

تعریف ۳.۲.۲. (**مارتین-لوف** [۳۰]). فرض کنید μ یک اندازه‌ی محاسبه‌پذیر باشد. $x \in 2^\omega$ نسبت به μ تصادفی است (و با $x \in R(\mu)$ نشان می‌دهند) هرگاه برای تمام آزمون‌های متوالی بازگشتی N نسبت به μ، $x \notin N$.

بدیهی است که $\mu(R(\mu)) = 1$؛ و می‌تواند نشان دهد که دنباله‌های تصادفی در این مفهوم (برای اندازه‌های به شکل $(1-p,p)^\omega$) قوانین احتمالات معمولی مانند قانون قوی اعداد بزرگ، قانون لگاریتم تکراری و ... را ارضا می‌کند. خاصیت زیر کمی تعجب‌آور است:

لم ۴.۲.۲. (***مارتین-لوف*** [۳۰]). *فرض کنید μ یک اندازه‌ی محاسبه‌پذیر باشد.*

(الف) مجموعه‌ی آزمون‌های متوالی بازگشتی نسبت به μ، شمارای کارآمد است.

(ب) یک آزمون متوالی بازگشتی جهانی نسبت به μ موجود است، به عنوان مثال Φ، به طوری که برای تمام آزمون‌های متوالی بازگشتی N نسبت به μ داشته باشیم $N \subseteq \Phi$.

یک نتیجه‌ی نادر از لم قبلی این است که $R(\mu)$ دارای عناصر نسبتاً ساده‌ای است. اگرچه آن شامل دنباله‌های بازگشتی نمی‌باشد اگر μ غیراتمی باشد، $R(\mu)$ شامل دنباله‌های Δ_2-تعریف‌پذیر نیست. این نتیجه‌ی حقیقت زیر است.

قضیه ۵.۲.۲. (***قضیه‌ی پایه‌ای سوآر***[۳] [۳۸]). *هر زیرمجموعه‌ی غیرخالی Π_1 از 2^ω دارای یک عضو Δ_2-تعریف‌پذیر است.*

[۳] Soare

برهان. (طرح). یک Π_1 زیرمجموعه از 2^ω می‌تواند به عنوان مجموعه‌ای از مسیرهای نامتناهی از میان درخت دودویی بازگشتی T در نظر گرفته شده باشد. $w \in T$ را قابل قبول گوییم هرگاه $\forall n > l(w)\ \exists v \in 2^n (w \subseteq v \& v \in T)$. (با استفاده از لم کونیگ[۴]، w قابل قبول است اگر و تنها اگر یک رشته‌ی نامتناهی از T از طریق w وجود داشته باشد.) مجموعه‌ی کلمه‌های قابل قبول Π_1 است. از آنجایی که زیرمجموعه غیر خالی است، T یک رشته‌ی نامتناهی دارد. سمت چپ‌ترین رشته‌ی نامتناهی می‌تواند به طور بازگشتی در مجموعه‌ی کلمات قابل قبول، که Π_1 است، ساخته شده باشد. بنابراین این رشته می‌بایست خودش Δ_2 باشد. □

لم زیر از اشنور[۵] [۳۵] منشاء گرفته است؛ یک برهان خلاصه را ارایه می‌دهیم.

لم ۶.۲.۲. *فرض کنید که μ یک اندازه‌ی محاسبه‌پذیر باشد. در اینصورت $R(\mu)$ شامل دنباله‌های Δ_2-تعریف‌پذیر است.*

برهان. با توجه به لم ۴.۲.۲، $R(\mu)$ یک Σ_2 مجموعه‌ی از اندازه‌ی 1 است. یک Π_1 مجموعه‌ی $A \subseteq R(\mu)$ را چنان انتخاب کنید که $\mu(A) > 0$ باشد و قضیه‌ی ۵.۲.۲ را اعمال کنید. □

ملاحظه ۷.۲.۲. *Ω شایتین Δ_2-تعریف‌پذیر است. برای فهمیدن نتیجه‌ی شایتین (قضیه‌ی D صفحه‌ی ۱۵۹ مرجع [۹])، به صورت زیر عمل می‌کنیم. فرض کنید $\lambda = (\frac{1}{2}, \frac{1}{2})^\omega$ و $x \in \Delta_2 \cap R(\lambda)$ باشد. با دلیل محکم‌تر، x، Π_2-تعریف‌پذیر است. چون هر رابطه‌ی شمارای کارآمد سیاله است [۱۲]، یک چندجمله‌ای P وجود دارد به طوری که*

$$\forall \overline{m} \exists \overline{k} P(\overline{m}, \overline{k}, n) = 0 \qquad \text{اگر و تنها اگر} \qquad x_n = 1 .$$

بنابراین می‌توان به شایتین گفت خواه ناخواه معادله‌ی $P(\overline{m}, \overline{k}, n) = 0$ یک راه حل برای تمام mها «در شیوه‌ای کاملاً غیرقابل پیش‌بینی به عنوان n تغییر به اطراف جهش می‌کند» را دارد. همانطور که دیدیم، یک ترکیب جزیی از تعدادی قضایای شناخته شده، نتیجه‌ی شایتین را تولید می‌کند. خواه این وضعیت به اندازه‌ی کافی توسط چنین تعابیری به عنوان «یک نسخه‌ی نمایشی از قضیه‌ی گودل»

[۴] König's Lemma

[۵] Schnorr

یا «قوی‌ترین نسخه‌ی ممکن از قضیه‌ی ناتمامیت گودل» [۹] شرح داده شده است، شاید یک امر سلیقه‌ای باشد. (یک کاربرد از ایده‌های نظریه‌ی الگوریتمی اطلاع در این زمینه بازدهی احتمالی این نتیجه است که محتوای اطلاع یک قضیه باید توسط ساده‌ترین اثباتش اندازه‌گیری شده باشد.) به هر حال، معتقدیم که مقایسه‌ی دینامیک غیرخطی و مکانیک کوانتومی نسبتاً بعید است. از آنجایی که در حالتی همچون حالات بالا ، به نظر می‌رسد یک محصول مصنوعی از تعریف انتخابی خاص را مشاهده می‌کنیم، لذا تصادفی بودن یک پدیده‌ی کوانتومی همچون چرخش الکترون‌ها، به محض اینکه تصمیم گرفتیم یک تعریف متناوب از تصادفی بودن را بپذیریم، از بین نمی‌رود. البته، تعاریف (حسابی) دیگر از دنباله‌های تصادفی، ساخته شده به کمک یک قضیه‌ی اساسی مناسب، مثال‌های جدیدی از «تصادفی بودن در ریاضیات» را به همراه خواهد داشت؛ اما برای مثال‌های فیزیکی که تحت تغییر تعریف ثابت می‌مانند، بیهوده به نظر می‌رسد. از این رو چیز نیرومندی که در مثال‌های فیزیکی که شایتین اشاره کرده است، در اینجا ناقص است.

۲.۲.۲ حاشیه

به عنوان یک صحبت فنی، در اینجا نشان می‌دهیم که دنباله‌های Δ_2-تعریف‌پذیر، حتی زمانی که تصادفی‌اند، رفتار پیچیده‌ی نسبتاً بی‌قاعده‌ای را ارایه می‌دهند، بنابراین بعضی حمایت‌ها برای محکومیت شهودی که چنین دنباله‌های ساده‌ای «واقعاً» نمی‌توانند تصادفی باشند. به عنوان یک امتیاز، یک برهان جدید از نتیجه‌ی مشهور مارتین-لوف را روی نوسانات پیچیدگی به دست می‌آوریم.

قضیه‌ی اول نوعی رفتار پیچیده از دنباله‌های دودویی نامتناهی را ارایه می‌دهد. اگر $x \in 2^\omega$، آنگاه $x(n)$ یک بخش ابتدایی از x به طول n و x_n، nامین مختص باشد.

در اینجا پیچیدگی کولموگروف به سه صورت مختلف زیر مطرح می‌شود:

جدول ۱.۲: پیچیدگی کولموگروف

نماد	تعریف
$K\mathbf{1}(s)$	طول کوتاهترین برنامه مولد s
$K\mathbf{2}(s)$	تعداد حالت‌های کوچکترین ماشین تورینگ مولد s
$K\mathbf{3}(s)$	کوچکترین اندیس تابع بازگشتی مولد s در نقطه 0

قضیه ۲.۲.۸. (*مارتین-لوف* [۳۰]). $\lambda\{x \in 2^\omega | \exists m \forall k \exists n \geq k \;\; K\mathbf{1}(x(n)) > n - m\} = 1$. *که در آن* $\lambda = (\frac{1}{2}, \frac{1}{2})^\omega$.

حال نشان می‌دهیم که دنباله‌های Δ_2-تعریف‌پذیر در این رابطه نسبتاً بی‌قاعده رفتار می‌کنند.

قضیه ۲.۲.۹. *اگر* $x \in 2^\omega$، Δ_2-*تعریف‌پذیر باشد، آنگاه* $\lim_{n\to\infty}(n - K\mathbf{2}(x(n))) = \infty$.

برهان. از لم استاندارد (سوآر [۳۸]) استفاده می‌کنیم: دنباله‌ی x در 2^ω، Δ_2 است اگر و تنها اگر برای برخی دنباله‌های $(\xi_k)_{k\in\mathbb{N}}$، Δ_2 باشد که در آن $\xi_k \in 2^\omega$ و مجموعه‌ی $\{\langle k, n\rangle | (\xi_k)_n = 1\}$ بازگشتی است: برای تمام nها، $x_n = \lim_{n\Rightarrow\infty}(\xi^k)_n$. (به عبارتی، دنباله‌های x، Δ_2-تعریف‌پذیر می‌توانند توسط ماشین‌های تورینگ تولید شده باشند اگر ماشین برای هر x_n مجاز به تنظیم خودش به تعداد متناهی بار باشد.) ابتدا نیازمند یک قرارداد روی کدگذاری رشته‌های دودویی هستیم. برای رشته‌های دوتایی w و v می‌توانیم دوتایی $\langle w, v\rangle$ را به یک رشته‌ی تکی $\underline{wv}$ به صورت زیر کد کنیم: دو بیت در wنوشتن یک 1 و سپس اضافه کردن v. یک الگوریتم A به صورت زیر تعریف می‌شود: A روی ورودی‌های به شکل $\underline{iq}$ عمل می‌کند که در آن i یک عدد طبیعی نوشته شده به صورت دودویی و q یک رشته‌ی دلخواه دودویی است. روی ورودی $\underline{iq}$، A ابتدا i و سپس $l(q)$ را مشخص می‌کند؛ سپس خروجی $A(\underline{iq}) = \xi^{i+l(q)}(i)q$ را می‌دهد. برای $l(q)$ به اندازه‌ی کافی بزرگ، $A(\underline{iq})$ به شکل زیر تعریف می‌شود:

$$A(\underline{iq}) = x(i)w \qquad \text{برای بعضی } w\text{ها،}$$

i را ثابت در نظر بگیرید، پس برای $n > i$ به اندازه‌ی کافی بزرگ داریم:

$$K(x(n)) \leq K_A(x(n)) + c \leq (n - i) + 2\log i + c.$$

بنابراین

$$\forall i \exists n_0 (i)_0 (i)\ (n - K(x(n)) \geq i - 2\log i - c).$$

چون طرف راست نامساوی بی‌کران است، لذا $\lim_{n\to\infty}(n - K(x(n))) = \infty$. □

قضیه ۲.۲.۱۰. (*مارتین-لوف* [۳۱]). $\forall x \forall m \exists n K\mathbf{3}(x(n)) \leq n - m$.

برهان. فرض (خلف) کنید که برای بعضی mها، $\{x|\forall nK\mathbf{3}(x(n)) > n - m\} \neq \emptyset$. با استفاده از قضیه‌ی ۵.۲.۲، این Π_1 مجموعه‌ی غیرخالی می‌بایست شامل یک عضو Δ_2-تعریف‌پذیر باشد، که در تناقض با قضیه‌ی قبلی است. □

برهان اصلی مارتین-لوف برای قضیه‌ی ۱۰.۲.۲ در اصل نتیجه‌ی ایده‌ی زیر است. فرض کنید $f : \omega \to 2^{<\omega}$ یک شمارش بازگشتی از $2^{<\omega}$ باشد. پس برای هر $x \in 2^{<\omega}$، تعداد نامحدودی بخش ابتدایی $x(n+i) = x(n)w$ که در آن $l(w) = i$، وجود دارد به طوری که $f(i) = x(n)$. شاید از این که قضیه‌ی ۱۰.۲.۲ همواره برای یک دلیل کاملاً متفاوت درست است، بهره می‌برد.

ملاحظه ۱۱.۲.۲. *در پایان، توجه داشته باشید که «تصادفی بودن در ریاضیات» حداقل از سال ۱۹۱۶ مورد بررسی قرار گرفته است، زمانی که وِیل[۶] اثبات کرد که برای α غیرمنطقی، دنباله‌ی $(n\alpha)_{n\in\omega}$ هم‌توزیع به مُد 1 است. مشکل عمومی این است که حتماً دنباله‌ی به سادگی تعریف شده تصادفی است، که در آن مفهوم تصادفی بودن در این فصل توسط محتوای آماری (به عنوان هم‌توزیع) و بدون استفاده از قضیه‌ی بازگشت مشخص شده است. مثال‌های دنباله‌های به سادگی تعریف شده که به شدت مشکوک به تصادفی بودن هستند:*

- *دنباله‌ای که nامین ترم آن 1 (0) است اگر و تنها اگر $(\frac{3}{2})^n$ به مُد 1 بزرگ‌تر از (کمتر از) $\frac{1}{2}$ باشد،*
- *دنباله‌ی $1 - 2$ کولاکوسکی[۷].*

اما کسی تاکنون قادر به اثبات آن‌ها نبوده است (به عنوان مثال [۳] و [۱۰] را مطالعه کنید).

مشاهده می‌شود که این دنباله‌ها بازگشتی هستند، بنابراین مطابق با تعاریف معمول غیرتصادفی‌اند. به هر حال، این علاقه‌ای از مسائل بالا کم نمی‌کند. دو راه برای وفق دادن تعاریف نظری تصادفی بودن با تمرین ریاضیدانان علاقه‌مند به این مفهوم، ظاهر می‌شود: یا به طور کلی پیچیدگی کولموگروف را بکار ببرد [۲۴] یا استفاده از قضیه‌ی بازگشت را در تعریف تصادفی بودن با هم مورد بررسی قرار دهد [۲۶].

---

[۶] Weyl

[۷] Kolakoski

فصل ۳

تفسیر قضیه ناتمامیت شایتین

نتیجه‌ی ناتمامیت نظریه-اطلاعی شایتین، یا به اختصار، قضیه‌ی شایتین، شاید یکی از مشهورترین و احتمالاً جاافتاده‌ترین نتایج منطق در پنج دهه‌ی اخیر باشد. قضیه‌ی شایتین بیان می‌کند که برای هر سیستم صوری $\mathbf{T}$، ثابت متناهی c چنان موجود است که $\mathbf{T}$ نمی‌تواند هیچ عبارتی به شکل «$K(w) > c$» را ثابت کند، حتی اگر تعداد نامتناهی w با خاصیت $K(w) > c$ وجود داشته باشند. در اینجا $K(w)$ پیچیدگی الگوریتمی، یا پیچیدگی محاسباتی w را نشان می‌دهد. قضیه‌ی شایتین توجه‌های زیادی را به خودش جلب کرده بود. دیویس[1] منطق‌دان برجسته و پیشگام نظریه‌ی بازگشتی، آن را «یک گسترش چشمگیر از نتیجه‌ی قضیه‌ی گودل» می‌نامد. نتیجه‌ی شایتین تعداد زیادی بحث درباره‌ی معنا و ارتباط فلسفی‌اش به وجود آورده است. تفسیر خود شایتین از نتیجه تقریباً از پذیرش جهانی برخوردار شده است. بر اساس این نظریه‌ی عامه، قضیه نشان می‌دهد که نظریه‌ی صوری نمی‌تواند یک شیء با پیچیدگی بیشتر از پیچیدگی خود نظریه را ثابت کند. فرض بر این است که پیچیدگی الگوریتمی اصول، یک معیار قوی، یا محتوای اطلاع نظریه را منعکس می‌کند.

هدف این فصل زیر سوال بردن این تفسیر است. در فصل قبل دیدیم که لامبالگن استدلال‌هایی برای همان نتیجه مطرح کرده است. اگرچه بحث وی دقیقاً نشان می‌دهد که باید اشتباهی در تفسیر عامه وجود داشته باشد، اما در واقع در مورد اینکه اشتباه کجاست چیزی نمی‌گوید. به علاوه، بحث درباره‌ی مسایل جدی را رها کرده است. دیدگاه عامه اتفاق در مقالات را ادامه می‌دهد، که ممکن است بدین معنی باشد که نقد لامبالگن به اندازه‌ی کافی ملموس نیست. هدفمان در اینجا این است که با ارایه مثال‌های نقض قوی‌تر، نقد را تقویت کرده و به طور قاطعانه نشان دهیم که دیدگاه عامه نادرست است. علاوه بر این، به مسایل معینی در خصوص ثابت محدود تعیین کننده‌ی قضیه‌ی مورد بحث در مقالات موجود پاسخ می‌دهیم. سعی می‌کنیم که ماهیت درستی از ثابت مشخصه را در مسایل مورد تجزیه و تحلیل قرار دهیم و ببینیم چه عاملی مردم را به چنین تفسیری سوق می‌دهد.

[1] M. Davis

۱.۳ برخی پیش نیازهای نظری بازگشت

ابتدا باید برخی مفاهیم پایه‌ای و نتایج قضیه‌ی بازگشت را که در ادامه استفاده شده‌اند مورد بررسی قرار دهیم. برای سادگی فرض می‌کنیم که یک عدد گذاری دوسویی از ماشین‌های تورینگ به $\mathbb{N}$ را داریم و ماشین‌های تورینگ را به صورت Φ_0 و Φ_1 و ... بشماریم؛ در اینجا از نمادگذاری راجرز [۳۲] برای مشخص کردن توابع بازگشتی جزیی متناظر با ϕ_0 و ϕ_1 و ... استفاده می‌کنیم. اگر ماشین تورینگ با کد m و با ورودی n متوقف شود، می‌نویسیم $\Phi_m(n)\downarrow$. تنها زمانی محاسبات را بدون ورودی نشان می‌دهیم که ورودی 0 باشد و بجای $\Phi_m(0)\downarrow$ می‌نویسیم $\Phi_m\downarrow$. اگر خروجی محاسبات روی y متوقف شود، آن را با $\Phi_m(n)\downarrow y$ و برای ورودی 0 با $\Phi_m\downarrow y$ مشخص می‌کنیم. هرگاه مقادیر ϕ_n و ϕ_m تعریف نشده باشند و یا اگر تعریف شده بودند برابر باشند، در این صورت می‌نویسیم $\phi_n \simeq \phi_m$. یک نتیجه‌ی اصلی از نظریه‌ی توابع بازگشتی توسط کلینی ارایه شد که مکراراً از آن به صورت زیر استفاده می‌کنیم:

قضیه ۱.۱.۳. (*قضیه‌ی نقطه‌ی ثابت*). *برای تابع بازگشتی داده شده‌ی f ، e چنان وجود دارد که e و $f(e)$ یک تابع را محاسبه می‌کنند، یعنی $\phi_e \simeq \phi_{f(e)}$.*

حقیقت اساسی وجود ماشین تورینگ جهانی Φ است، ماشینی که اگر عدد کد e از ماشین‌های تورینگ و عدد n را به عنوان ورودی به آن بدهیم، همانند محاسبات ماشین تورینگ Φ_e روی n عمل کند، یعنی $\Phi(e,n) \simeq \Phi_e(n)$. برای سادگی ملاحظات زیر، فرض می‌کنیم که می‌توانیم دو ورودی Φ را الحاق کرده و یک ورودی به طول $e+n$ داشته باشیم. اجازه دهید ارزش شبیه‌سازی ماشین تورینگ Φ_e با ورودی n، یعنی $\Phi_e(n)$، توسط ماشین تورینگ جهانی را با e که کد همان ماشین تورینگ شبیه‌سازی شده است نشان دهیم.

در ادامه مفهوم اندیس قابل قبول را تعریف می‌کنیم که توسط راجرز ارایه شده است. کدگذاری «معمول» ϕ_e، کدگذاری استاندارد نامیده می‌شود. هر سیستم از اندیس‌ها، خانواده ψ از توابع ψ^n از ω به مجموعه‌ی توابع بازگشتی جزیی nموضعی است. معمولاً می‌توان ذکر تعداد متغیرها را از قلم انداخت.

تعریف ۲.۱.۳. یک سیستم A از اندیس‌ها، قابل قبول نامیده می‌شود هرگاه توابع بازگشتی تام g و f چنان موجود باشند که $A_e \simeq \phi_{f(e)}$ و $\phi_e \simeq A_{g(e)}$.

بنابراین یک سیستم قابل قبول است هرگاه بتواند به طور کارآمد از کدگذاری استاندارد به سیستم برود و برعکس. راجرز نشان داده بود که سیستم اندیس‌ها قابل قبول است اگر و تنها اگر آن هم شمارش و هم پارامتری‌سازی را ارضا کند، و اینکه هر سیستم قابل قبول از اندیس‌ها قضیه‌ی نقطه‌ی ثابت را ارضا کند. از این روی می‌توان گفت که سیستم‌های قابل قبول از اندیس‌ها همان ساختار نظریه را برای توابع بازگشتی به صورت استاندار فراهم می‌کند. بنابراین، از نقطه نظر محاسبه‌پذیری، در حقیقت هیچ تفاوتی در اینکه کدام سیستم قابل قبول از اندیس‌ها بکار بسته می‌شوند را به وجود نمی‌آورد.

۲.۳ قضیه‌ی ناتمامیت شایتین

در ابتدا می‌بایست تعریفی از پیچیدگی کولموگروف، یا پیچیدگی الگوریتمی، را ارایه داده و به قضیه‌ی شایتین بپردازیم.

تعریف ۱.۲.۳. پیچیدگی الگوریتمی x، که با $K(x)$ نشان می‌دهیم، به صورت زیر تعریف می‌شود:

$$K(x) = \mu e(\phi_e(0) \simeq x)،$$

یعنی کوچکترین e که $\phi_e(0) \simeq x$.

در حقیقت تعاریف متفاوت زیادی در مقالات وجود دارد اما این فصل منحصراً با قضیه‌ی ناتمامیت شایتین سروکار دارد که ظرافت‌های نظریه‌ی الگوریتمی اطلاع ما را اذیت نمی‌کند، از این رو تعریف ساده‌ی فوق برای این منظور کافی است.

توجه کنید که $\phi_x(0) \simeq y$ به عنوان رابطه‌ی شمارای کارآمد، یا Σ_1^0، مطرح شده است. پیچیدگی الگوریتمی $K(x) = y$ به صورت $\phi_y(0) \simeq x \;\&\; \forall z < y(\neg\phi_z(0) \simeq x)$ تعریف شده است و از این رو $K(x) = y$ به عنوان یک رابطه، Σ_2^0 است.

در ادامه، فرض می‌شود که سیستم صوری $\mathbf{T}$ به طور بازگشتی اصل‌پذیر و به اندازه‌ی کافی قوی است (شامل حساب رابینسون[۲] $\mathbf{Q}$ بوده و یا $\mathbf{Q}$ بتواند در آن تعبیر شود). به علاوه، فرض می‌شود که $\mathbf{T}$ نظریه‌ی صحیح است، یعنی قضایای آن (حداقل قضایایی که به شکل «$K(x) > y$» هستند) درست هستند. با رسمیت بیشتر، این می‌تواند توسط اصل انعکاس $Prov_{\mathbf{T}}(\ulcorner K(x) > c \urcorner) \Rightarrow K(w) > c$ مطرح شود.

اثبات حسابی شده‌ی مبتنی بر $\mathbf{T}$، بیان می‌کند که «x عدد گودل یک اثبات در نظریه‌ی $\mathbf{T}$ برای فرمولی با عدد گودل y است» و به اختصار با $Prf_{\mathbf{T}}(x, y)$ نمایش می‌دهیم. گزاره‌ی اثبات‌پذیری $Prov_{\mathbf{T}}(y)$ به صورت $\exists x Prf_{\mathbf{T}}(x, y)$ تعریف شده و به صورت «فرمولی با عدد گودل y در $\mathbf{T}$ اثبات‌پذیر است» بیان می‌شود.

حال آماده‌ی بیان قضیه‌ی ناتمامیت شایتین و بحث درباره‌ی راه‌های متفاوت اثبات آن می‌باشیم.

قضیه ۲.۲.۳. (*قضیه‌ی شایتین*). *برای هر نظریه‌ی صوری شده‌ی (به اندازه‌ی کافی قوی) $\mathbf{T}$، ثابت c چنان وجود دارد که $\mathbf{T}$ برای تمام wها، $K(w) > c$ را اثبات نمی‌کند.*

برهان. (طرح برهان). فرض کنید Φ_m ماشین تورینگی باشد که به صورت زیر عمل می‌کند:

«اگر برای w، کوچکترین xای را یافت که $\Phi_m = ، Prf_{\mathbf{T}}(x, \ulcorner K(w) > c \urcorner)$
آنگاه w را چاپ کند.»

اجازه دهید که عدد c را طوری انتخاب کنیم که $c > m$. تنها چیز مهم این است که c عدد بزرگی است ولی با این وجود می‌تواند توسط یک زیر برنامه‌ی ساده که از اندازه‌ی ماشین تورینگ بزرگ‌تر نیست، تولید شده باشد.

می‌توان نشان داد که Φ_m متوقف نمی‌شود (و بنابراین، برای تمام wها، $\mathbf{T}$، $K(w) > c$ را اثبات نمی‌کند). فرض (خلف) کنید که $\Phi_m \downarrow$. در اینصورت با فرض صحت، $\Phi_m \downarrow w \Rightarrow K(w) > c$. از طرف دیگر، با توجه به تعریف $K(w)$ و فرض اینکه $c > m$، $\Phi_m \downarrow w \Rightarrow K(w) \leq m$؛ بنابراین، $K(w) < c$ که یک تناقض است. □

[۲] Robinson-Arithmetic

۱.۲.۳ ایده‌ی اثبات

مشابه برهان گودل، این برهان یک استفاده‌ی مثبت از یک پارادوکس را می‌سازد. نقل قول خود شایتین:

> این برهان شباهت زیادی به پارادکس بری[۳] دارد که «کوچکترین عدد طبیعی که در کمتر از 10000000 کلمه قابل توصیف نیست» (اما این عدد در 12 کلمه توصیف شده است!) ... نسخه‌ای از پارادکس بری که با این ترفند انجام خواهد گرفت «که شیء دارای کوتاه‌ترین برهانی است که محتوای الگوریتمی اطلاع آن بزرگ‌تر از یک میلیون بیت است» ...

وی در متن دیگری قضیه‌اش را به صورت زیر توضیح می‌دهد:

> نتیجه ... برنامه‌ی محاسباتی زیر است: «یک سری از ارقام دودویی را پیدا کن که بتواند وجود پیچیدگی بزرگ‌تر از تعداد بیت‌های این برنامه را ثابت کند.» برنامه تمام برهان‌های ممکن در سیستم صوری را به ترتیب اندازه‌هایشان تا زمانی که با اولین اثباتی که یک دنباله‌ی دودویی خاص با پیچیدگی بزرگ‌تر از تعداد بیت‌های برنامه دارد برخورد کند. آنگاه دنباله‌ها را چاپ کرده و متوقف می‌شود. ... برنامه به طور فرضی عددی را نتیجه می‌دهد که هیچ برنامه‌ای با اندازه‌اش نباید قادر به نتیجه‌گیری باشد. ... پوچی این نتیجه گیری فقط شرح می‌دهد که برنامه هیچ‌گاه عددی را که در جستجوی آن بوده را نخواهد یافت ...

ایده‌ی طرح برهان فوق به برهان‌های ارایه شده توسط دیویس[۴] و بولوس[۵] کاملاً نزدیک است. به هر حال، یک شکاف ناخوشایند در این برهان وجود دارد. یعنی، فرض می‌شود که فقط می‌توان یک عدد c را انتخاب کرد که نیازمان را ارضا می‌کند، اما این به عنوان یک اصل از اعتقادمان را رها کرده است. در ادامه دو راه برای کامل کردن این برهان مطرح می‌کنیم.

---

[۳] Berry's Paradox

[۴] Davis

[۵] Boolos

۲.۲.۳ ساختار نقطه ثابت

در حال حاضر ویژگی خودارجاع از ماشین تورینگ نشان می‌دهد که می‌توانیم با اعمال قضیه‌ی نقطه‌ی ثابت کلینی[۶] یک عدد مناسب پیدا کنیم. درواقع این اولین راه کامل کردن برهان است.

برای عدد c داده شده می‌توان (یک عدد کد از) ماشین تورینگ Φ_m را یافت که به صورت تعریف فوق عمل می‌کند. اجازه دهید تابع بازگشتی که m را به c نظیر می‌کند را با f مشخص کنیم، یعنی $f : c \to m$. حال با استفاده از قضیه‌ی نقطه‌ی ثابت می‌توان به طور کارآمد عدد e را یافت که $\Phi_e \simeq \Phi_{f(e)}$. با توجه به تعریف

$$\Phi_{f(e)} = \text{«اگر برای } w\text{، کوچکترین } x\text{ای را یافت که } (Prf_{\mathbf{T}}(x, \ulcorner K(w) > e \urcorner\text{،}$$
$$\text{آنگاه } w \text{ را چاپ کند.»}$$

چون $\Phi_e \simeq \Phi_{f(e)}$ لذا

$$\Phi_e = \text{«اگر برای } w\text{، کوچکترین } x\text{ای را یافت که } (Prf_{\mathbf{T}}(x, \ulcorner K(w) > e \urcorner\text{،}$$
$$\text{آنگاه } w \text{ را چاپ کند.»}$$

بنابراین، به طور کارآمد e را یافتیم که کلک می‌زند.

۳.۲.۳ ساختار شایتین

خود شایتین از یک روش متفاوت برای ساختن ثابت مشخصه‌اش استفاده کرده است. وی برهان‌های متفاوتی از نتیجه‌اش را منتشر کرده است. حال توصیفی که از ایده‌ی اصلی برهان‌هایش ارایه می‌دهیم کمی منصفانه‌تر است. واضح است که اجزاء ظریف یا ساده شده و یا از قلم انداخته‌ایم. ابتدا می‌توان $K_\Phi(n)$، پیچیدگی الگوریتمی عدد (رشته) n وابسته به یک ماشین تورینگ Φ را تعریف کرد که اندازه‌ی کوتاه‌ترین برنامه‌ای (ورودی) است به طوری که وقتی به Φ داده می‌شود n را تولید کند. به وضوح ممکن است K_Φ در تعداد زیادی از حالت‌ها برخی یا تمام اعداد را بدون تعیین پیچیدگی از قلم بیاندازد. در ادامه‌ی همین بحث، شایتین یک ماشین تورینگ جهانی Φ که می‌تواند مشابه

[۶] Kleene's Fixed-Point Theorem

هر ماشین تورینگ عمل کند را در نظر می‌گیرد. پیچیدگی الگوریتمی «مطلق» به صورت پیچیدگی الگوریتمی نسبت به یک چنین ماشین تورینگ جهانی تعریف شده است.

لم مهم زیر برهان شایتین را ایجاب می‌کند:

لم ۳.۲.۳. *برای هر ماشین تورینگ Φ و هر عدد n، $K(n) \leq K_\Phi(n) + c$ که در آن ثابت c کد ماشین تورینگ Φ است.*

در ادامه یک هدف خاص ماشین تورینگ Φ به صورت زیر تعریف می‌شود: ماشین تورینگی که ورودی‌هایش دوتایی‌های مرتب $(\ulcorner A \urcorner, k)$ است که در آن A یک الحاق از اصول نظریه‌ی صوری شده‌ی مورد بحث و k یک عدد است. Φ را در نظر بگیرید که به صورت زیر عمل می‌کند:

«اگر برای w، کوچکترین xای را یافت که $Prf(x, \ulcorner K(w) > c \urcorner)$، $\Phi =$
که در آن $c = \ulcorner A \urcorner + 2k$، آنگاه w را چاپ کند.»

می‌توان در ادامه اصول A را ثابت در نظر گرفت و بررسی کرد که کد این ماشین تورینگ Φ چیست. اجازه دهید کد این ماشین تورینگ را با n نشان دهیم. اگر Φ متوقف شود، پیچیدگی w نسبت به Φ، یعنی $K_\Phi(w)$، با تعریف پیچیدگی نسبی کمتر و یا مساوی $(\ulcorner A \urcorner + k)$ است. توجه کنید که n، به عنوان کد Φ، ارزش شبیه‌سازی Φ توسط ماشین تورینگ جهانی است. از اینرو، با توجه به لم ۳.۲.۳، پیچیدگی «مطلق» $K(w) \leq (\ulcorner A \urcorner + k) + n$. در ادامه n را به عنوان ورودی دوم برای Φ، یعنی $k = n$، وارد می‌کنیم. بنابراین اگر Φ متوقف شود، برهانی (از A) را برای $K(w) > c$ پیدا خواهد کرد که در آن $c = \ulcorner A \urcorner + 2n$. با فرض صحت، این همان c تعریفِ Φ است. بنابراین، از یک طرف $K(w) > \ulcorner A \urcorner + 2n$، و از طرف دیگر چون $k = n$ و همانگونه که ذکر شد $K(w) \leq (\ulcorner A \urcorner + k) + n$ لذا $K(w) \leq \ulcorner A \urcorner + 2n$ که یک تناقض است. از اینرو Φ نمی‌تواند متوقف شود و برای تمام wها نمی‌تواند برهانی (از A) برای $K(w) > c$ یافت شود که در آن $c = \ulcorner A \urcorner + 2n$.

۴.۲.۳ مقایسه‌ی دو روش

اگرچه روش شایتین برای نتیجه‌اش مستقیم نیست، اما باید قبول کرد که روش شایتین از جمله روش‌های هوشمندانه به شمار می‌رود. این روش از هرگونه خودارجاعی مستقیم اجتناب می‌کند و از اینرو نیازی به استفاده از قضیه‌ی نقطه ثابت یا برخی از نتایج پیشرفته نظیر توابع بازگشتی، که ممکن است برخی در درک آن‌ها مشکل داشته باشند، ندارد. در عوض، تنها ایده‌های قابل فهم از یک ماشین تورینگ جهانی و ارزش شبیه‌سازی یک ماشین تورینگِ هدف خاص مورد نیاز است. از طرف دیگر، این روش ممکن است برای یک منطق‌دان با دانش خوب از نظریه توابع بازگشتی، پیچیدگی بی ارزشی به نظر برسد. به عنوان یک نتیجه‌گیری، این مقایسه قادر است که بگوید آن روش‌ها ماهیتی از یک سلیقه‌ی شخصی است که طریقه‌ی یافت یک ثابت معین مناسب را برمی‌گزینند.

۳.۳ تفسیر عامه از نتیجه‌ی شایتین

همانطور که گفته شده بود، قضیه‌ی شایتین موجب ایجاد بحث‌های بسیار زیادی درباره‌ی مفهوم ارتباط فلسفی‌اش شده بود. تفسیر مورد علاقه‌ی خود شایتین به دیدگاه عامه روی موضوع و تکرار صادقانه در مقالات تبدیل شده بود. نقل قول زیر از نگارش شایتین به نظر کاملاً قابل درک است:

> ... من می‌خواهم به اندازه‌گیری قدرت یک مجموعه از اصول و قوانین استنتاج بپردازم. می‌خواهم قادر به بیان این موضوع باشم که اگر کسی ده کیلو اصول و بیست کیلو قضیه داشته باشد، آنگاه قضیه نمی‌تواند از این اصول مشتق شده باشد.
>
> چون پیچیدگی به عنوان اندازه‌ای از تصادفی بودن تعریف شده بود، این قضیه بیان می‌کند که در یک سیستم صوری، عدد گودل هیچ فرمولی نمی‌تواند به صورت تصادفی ثابت شده باشد مگر اینکه پیچیدگی آن عدد کمتر از پیچیدگی خود سیستم باشد.
>
> ... آن ممکن است اثبات کند که یک شیء خاص با پیچیدگی بزرگ‌تر از n است فقط اگر n کوچک‌تر از پیچیدگی اصول به کار رفته در اثبات باشد. ...
>
> اندازه‌گیری قدرت نظریه‌های صوری حساب در ترم‌های نظریه-اطلاعی معقول به نظر

می‌رسد ...

هیچ تعداد بیتی در خود برنامه که عامل محدود کننده باشد وجود ندارد اما تعداد بیت‌ها در سیستم صوری به صورت یک مجموع است. در برنامه، اصول و قواعد استنتاجی که رفتار سیستم را مشخص کرده و الگوریتمی برای آزمایش برهان‌ها ارایه کند، پنهان است. ... بنابراین اندازه‌ی برنامه‌ی بی‌عیب از پیچیدگی سیستم‌های صوری با یک تعداد بیت ثابت c تجاوز می‌کند. (مقدار حقیقی c به زبان ماشین به کار رفته بستگی دارد.) بنابراین قضیه‌ی اثبات شده با پارادکس می‌تواند به صورت زیر بیان شده باشد: در یک سیستم صوری با پیچیدگی n ممکن است اثبات کند که یک سری از ارقام دودویی، از پیچیدگی بزرگ‌تر از $n + c$ است که در آن c ثابتی است که قطع نظر از سیستم خاص به کار گرفته شده است.

۱.۳.۳ خلاصه‌ای از تفسیر عامه

حال باید سعی بر تکرار و تعیین محتوای اصلی این تفسیر داشته باشیم. ابتدا در پیرو لامبالگن، می‌بایست کوچکترین c که برای تمام wها، سیستم صوری $\mathbf{T}$ قادر به اثبات $K(w) > c$ نیست را ثابت مشخصه‌ی سیستم صوری $\mathbf{T}$ نامیده و آن را با $c_{\mathbf{T}}$ نشان می‌دهیم. این نکته برای آنالیز تفسیر عامه شامل دو بخش مفید زیر است:

(۱) می‌توان قدرت، یا محتوای اطلاع، نظریه‌ی صوری حسابی را با استفاده از پیچیدگی الگوریتمی اصول (یا در بعضی مواقع، اصول و قواعد استنتاج با هم پیشنهاد شده است) اندازه‌گیری کرد.

(۲) ثابت محدود $c_{\mathbf{T}}$ (همان ثابت مشخصه‌ی $\mathbf{T}$) فقط به پیچیدگی اصول $\mathbf{T}$ بستگی دارد.

این دو با هم اشاره‌ی مشابهی به این که ثابت مشخصه‌ی یک نظریه به طریقی قدرت نظریه را منعکس می‌کند، دارند. لازم به ذکر است که در قسمت (۲) چند ابهام وجود دارد: بعضی مواقع بیان می‌کند که آن طول اصول مربوطه است، گاهی پیچیدگی اصول و گاهی اندازه‌ی پیچیدگی اصول و قواعد استنتاج را با هم در نظر می‌گیرد. به هر حال، در نقد ما هر دو این گزینه‌ها اعمال خواهد شد.

۲.۳.۳ نقد تفسیر عامه

همانطور که اشاره شد، لامبالگن از این دیدگاه عامه انتقاد کرده بود. وی بیان می‌کند که این تفسیر «در حال حاضر فقط بخش خیلی کمی توسط حقایق پشتیبانی شده است». سپس او به نتیجه‌ای از کریزل و لوی اشاره کرده و استدلال می‌کند که تعداد بی‌نهایت نظریه‌ی اعداد قوی $\mathbf{T}_n$، وجود دارند که بین **PA** و **ZF** قرار داشته و همان ثابت مشخصه‌ی c را دارا می‌باشند. لامبالگن تاکید می‌کند که «ما حتی نمی‌دانیم که آیا $c_{\mathbf{ZF}} > c_{\mathbf{PA}}$ ... ! و بدتر از این، ما حتی هیچ ایده‌ای درباره‌ی نحوه‌ی تصدیق نتایجی از این نوع نداریم.» ما با این نکات اساسی موافقیم ولی باید نشان دهیم که بیشتر از این‌ها می‌توان درباره‌ی این موضوع صحبت کرد. زمانی که خواننده به آخر فصل قبل می‌رسد پی می‌برد که نه تنها تفسیر عامه «در حال حاضر فقط بخش خیلی کمی توسط حقایق پشتیبانی می‌شود»، بلکه به طور کامل در تضاد با حقایق است. ابتدا، مثال‌های نقض قوی را برای دیدگاه عامه ارایه می‌دهیم. بحثمان نشان می‌دهد که پرسش قبلی لامبالگن، یعنی $c_{\mathbf{ZF}} > c_{\mathbf{PA}}$ و نحوه‌ی تصدیق نتایجی از این نوع، خوشتعریف نیست.

۴.۳ چگونه ثابت مشخصه را صفر کنیم؟

به عنوان یک کاربرد سرگرم کننده از قضیه‌ی نقطه ثابت، نشان می‌دهیم که چگونه در هر نظریه‌ی صوری ثابت مشخصه صفر می‌شود.

قضیه ۱.۴.۳. *برای هر نظریه‌ی صوری $\mathbf{T}$، امکان تعریف سیستم قابل قبولی از اندیس‌ها وجود دارد که ثابت مشخصه $c_{\mathbf{T}} = 0$ می‌شود.*

برهان. اجازه دهید سیستم صوری $\mathbf{T}$ را شامل حساب ابتدایی در نظر بگیریم که برای اثبات قضیه می‌خواهیم. فرض کنید که کدگذاری دوسویی اولیه π از ماشین‌های تورینگ به اعداد طبیعی داده شده: بنابراین ماشین‌های تورینگ می‌توانند به صورت Φ_0 و Φ_1 و ... شمارش شده باشند. و اجازه دهید تابع رمزگزین π^n (نسبت به n داده شده) را به صورت زیر تعریف کنیم:

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

واضح است که برای کدگذاری اولیه π و عدد n داده شده، می‌توان به طور کارآمد کدگذاری جدید تعیین شده توسط π^n را به دست آورد. پیچیدگی کولموگروف را نسبت به این کدگذاری جدید K^n می‌نامیم، یعنی $K^n(x) = \mu z\big(\exists y[\pi^n(y) = z \wedge \Phi_y \downarrow x]\big)$. پیچیدگی الگوریتمی حسابی است و می‌توان یک فرمول صوری که آن را (برای کدگذاری اولیه) تعریف می‌کند ساخت. پس برای این فرمول داده شده، به سادگی با استفاده از صوری‌سازی تعریف فوق برای π^n، می‌توان به طور کارآمد فرمولی پیدا کرد که برای n داده شده K^n را تعریف کند. به علاوه، برای عدد گودلِ فرمول داده شده، می‌توان به طور کارآمد عدد گودلِ فرمول اخیر را پیدا کرد. می‌توان به طور کارآمد ماشین تورینگ Φ_m (که رمز آن از کدگذاری اولیه m است) یافت که حداقل xای را جستجو کند که برای بعضی pها، $Prf_{\mathbf{T}}\big(x, \ulcorner K^n(p) > 0 \urcorner\big)$، 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 اولیه‌اش 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، (عدد گودلِ) برهانی از فرمولی 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. و e را عدد رمز (اولیه) این برنامه در نظر بگیرید.» با رسمیت بیشتر، این خودارجاعی می‌تواند به صورت زیر به کار گرفته شده باشد: تابع بازگشتی $f(x)$ وجود دارد به طوری که برای عامل n داده شده در K^n، $f(n) = m$ عدد رمز (اولیه) ماشین تورینگی که در بالا توصیف کردیم است. با استفاده از قضیه نقطه ثابت، عدد eای وجود دارد به طوری که Φ_e و $\Phi_{f(e)}$ تابع یکسانی را محاسبه می‌کنند. به علاوه، برهان قضیه نقطه ثابت تنها 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، 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، برنامه‌ی با عدد رمز 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 رمز Φ_e می‌باشد. اما در کدگذاری تعیین شده با π^n رمز 0 است ($\pi^e(e) = 0$) و لذا $K^e(p) = 0$. از طرف دیگر اثبات $K^e(p) > 0$ را داشتیم. با فرض صحت، $K^e(p) > 0$ درست است. بنابراین به تناقض رسیدیم. □

۱.۴.۳ نتیجه

توجه داشته باشید که اگر این ساختار را برای سیستم‌های قوی، برای مثال نظریه‌ی مجموعه تسرملو-فرانکل[۷]، به اختصار **ZFC**، اعمال کنیم و کدگذاری ماشین تورینگ ثابت باشد، ثابت مشخصه‌ی هر نظریه‌ی صوری صحیح، از ضعیف‌ترین حساب ابتدایی (به عنوان مثال **Q** رابینسون[۸]) تا **ZFC**، همان مقدار صفر را خواهد داشت. این نشان می‌دهد که تحت برخی کدگذاری‌های قابل قبول، ثوابت مشخصه‌ی نظریه‌های دارای قدرت‌های اساساً متفاوت، خواه اندازه‌گیری توسط قدرت برهان نظری صورت گرفته باشد خواه توسط پیچیدگی الگوریتمی اصول، ممکن است مقدار یکسانی باشد.

۵.۳ چگونه ثابت مشخصه را به طور دلخواه بزرگ کنیم؟

می‌توان به سادگی موقعیتی فراهم کرد که «ثابت مشخصه» یک سیستم صوری به طور دلخواه بزرگ شود. این ساختار به وضوح نشان می‌دهد که یک نظریه ممکن است به خوبی عددی را که دارای پیچیدگی بزرگتر از پیچیدگی نظریه است را ثابت کند. صرفاً یک طرح از این ایده را ارایه می‌دهیم.

۱.۵.۳ ساختار

فرض کنید که **T** یک نظریه‌ی صوری شده‌ی شامل حساب ابتدایی باشد. فرض کنید که Φ ماشین تورینگی باشد که اصول **T** را چاپ کرده و متوقف می‌شود. ماشین تورینگ جهانی را طوری در

[۷] Zermelo-Fraenkel Set Theory

[۸] Robinson

نظر می‌گیریم که کد ماشین تورینگ مذکور 1 باشد. و فرض کنید که $\mathbf{T}$ به قدر کافی قوی است که می‌تواند ثابت کند Φ اصول $\mathbf{T}$ را چاپ کرده و متوقف می‌شود.

حالت اولیه با I_Φ نشان داده شده است. ماشین تورینگ بعدی را به صورت $q_1 00 q_1$ در نظر بگیرید. چون دستور این ماشین تورینگ فاقد حالت اولیه است پس واضح است که این ماشین تورینگ حتی شروع به کار نمی‌کند و این حقیقت بدیهی در هر نظریه صوری شامل حساب ابتدایی قابل اثبات است. حال یک کدگذاری را به طریق زیر تعیین کنید: کد 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 هر نظریه‌ی صوری شده‌ی شامل حساب ابتدایی قابل اثبات است. بنابراین، ما می‌توانیم $K(1) > n$ را در $\mathbf{T}$ ثابت کنیم. لذا، ثابت مشخصه‌ی نظریه $\mathbf{T}$، $c_\mathbf{T}$، می‌بایست بزرگ‌تر از n باشد. با توجه به ساختار فوق، پیچیدگی اصول $\mathbf{T}$ تحت این کدگذاری 1 است. لذا تحت این کدگذاری، $\mathbf{T}$ می‌تواند قضیه‌ای را اثبات کند که پیچیدگی بیشتری از اصول خودش دارد. پس به این ترتیب، تعبیر عمومی از نتیجه شایتین، که $c_\mathbf{T}$ محتوای اطلاع یا میزان قدرت نظریه صوری $\mathbf{T}$ را اندازه‌گیری می‌کند و $\mathbf{T}$ نمی‌تواند ثابت کند هیچ شیئی با پیچیدگی کولموگروف بیشتر از $c_\mathbf{T}$ وجود دارد، رد می‌شود.

۶.۳ منبع واقعی ثابت مشخصه

ملاحظات فوق نشان می‌دهد که مقدار ثابت مشخصه‌ی نظریه‌ی صوری شده قدرت یا محتوای اطلاع اصول را منعکس نمی‌کند. ممکن است این سوال پیش آید که منبع واقعی ثابت مشخصه چیست؟ راتیکاینن معتقد بود که می‌توان یک پاسخ دقیق به این سوال ارایه کرد. این تفکر نشان می‌دهد که مقدار $c_\mathbf{T}$ در حقیقت توسط کوچک‌ترین (کد) ماشین تورینگی تعیین می‌شود که متوقف نمی‌شود و متوقف نشدن آن نمی‌تواند در $\mathbf{T}$ اثبات شود. کوچک‌ترین e را در نظر بگیرید که $\neg\exists x \phi_e \simeq x$

درست است اما نمی‌توان در سیستم صوری داده شده‌ی $\mathbf{T}$ آن را ثابت کرد. ممکن است برای هر m و هر $e < n$، در $\mathbf{T}$ ثابت کند که $\phi_n(0) \simeq m \,\&\, \forall z < n \neg\phi_z(0) \simeq m$، زیرا در $\mathbf{T}$ امکان اینکه e یک چنین zای باشد را نمی‌توان رد کرد. نمی‌توان ثابت کرد که هر عدد خاص پیچیدگی بزرگ‌تر از e دارد. مشاهده‌ی اینکه چرا کد یک چنین ماشین تورینگی که همه چیز را در مورد «قدرت» یا «محتوای اطلاع» نظریه‌ی صوری $\mathbf{T}$ آشکار می‌کند واقعاً سخت به نظر می‌رسد. توجه کنید ممکن است (همانند توضیحات فوق، و همچنین استدلال‌های لامبالگن، نشان دهد) که نظریه‌های با قدرت متفاوت این ثابت متعارف را داشته باشند.

به هر حال، توجه داشته باشید که این مشاهدات برهان تقریباً بدیهی قضیه‌ی شایتین، که با توجه به این حقیقت معروف که هیچ سیستم صوری نمی‌تواند تمام جملات درست به شکل $\neg\exists x \phi_e(0) \simeq x$ را ثابت کند، را فراهم می‌کند.

۷.۳ درهم‌آمیختگی کارکرد و نقل قول

در تحلیلمان از تفسیر عامه، این ادعا «که قدرت یا محتوای اطلاع یک سیستم صوری توسط پیچیدگی اصولش (یا پیچیدگی اصول و قواعد استنتاجش) اندازه‌گیری می‌شود» را رد می‌کنیم. در ادامه باید درباره‌ی اینکه این ادعا بشدت غیرمحتمل است و به احتمال زیاد اساس این ادعا درهم‌آمیختگی نقل قول و کارکرد است، بحث کنیم.

برای شروع، مفهوم نظریه برهان مفروض از قدرت را به این صورت می‌پذیریم که نظریه‌ی $\mathbf{T}_1$ قوی‌تر از نظریه‌ی $\mathbf{T}_2$ است، هرگاه $\mathbf{T}_1$ تمام قضیه‌هایی را که $\mathbf{T}_2$ ثابت می‌کند را ثابت کند. حقیقتاً تفکر جدی درباره‌ی تمام مفاهیم توان، قدرت یا محتوای اطلاع نظریه‌ای که این مفهوم طبیعی را نقض کند، سخت است. اما ایده‌ی اندازه‌گیری آن‌ها توسط پیچیدگی اصول به وضوح مغایر با این تصویر شهودی است. یک نظریه‌ی ضعیف ممکن است پیچیده‌تر از یک نظریه قوی شامل آن باشد.

به عنوان یک مثال ساده مضحک، نظریه‌ی $\mathbf{T}_1$ بسیار بزرگ و مجموعه‌ی متناهی فوق‌العاده پیچیده (نسبت به کد گذاری داده شده) از معادلات به شکل $n = n$ را در نظر بگیرید. حال مطابق با تفسیر عامه، این نظریه دارای قدرت بیش ازحد و حاوی اطلاعات مفیدی است. اما البته، در حقیقت این

نظریه خیلی ضعیف و کاملا بی‌فایده است. این نظریه مشمول نظریه‌ی خیلی ساده و بدیهی $\mathbf{T}_2$ است که شامل تنها اصل $\forall x(x = x)$ می‌باشد.

همچنین به نظر می‌رسد اصول حساب بازگشتی ابتدایی **PRA** پیچیده‌تر از اصول نظریه‌ی مجموعه‌ی تسرملو-فرانکل **ZFC** باشد، اما ارایه‌ی مفهومی که ادعا کند **PRA** قوی‌تر، یا دارای محتوای اطلاع بشتر از **ZFC** است، سخت به نظر می‌رسد. به بیان ساده، قدرت، یا محتوای اطلاع یک نظریه کاملا مستقل از مشکل نحوه‌ی بیان آن است.

این‌گونه تصور می‌شود که نمونه روشنی از درهم‌آمیختگی بین کارکرد و نقل قول وجود دارد، تمایزی که دارای اهمیت ویژه‌ای است، توسط کواین[۹] تاکید شده است. وی به خوبی این تمایز را با این مثال که بستون (کلمه‌ی مورد استفاده) 800000 نفر جمعیت دارد، اما «بستون» (کلمه‌ی مذکور) شامل پنج حرف است، نشان داده است.

۸.۳ قدرت و ثوابت مشخصه‌ی نظریه‌ها

در بخش ۶.۳ نشان دادیم که در حقیقت مقدار یک ثابت مشخصه توسط کوچک‌ترین ماشین تورینگی که متوقف نمی‌شود و نمی‌توان توقف ناپذیری آن را ثابت کرد تعیین می‌شود. در ادامه مثالی می‌آوریم که مشکل تفسیر عامه را روشن می‌سازد.

نظریه‌ی $\mathbf{T}$ را با ثابت مشخصه c در نظر بگیرید. می‌توان دو توسیع برای $\mathbf{T}$ به صورت $\mathbf{T}_1$ و $\mathbf{T_2}$ در نظر گرفت به طوری که به $\mathbf{T}_1$ جمله (درست) که «Φ_c متوقف نمی‌شود» را اضافه می‌کنیم، و به $\mathbf{T}_2$ یک جمله‌ی مشابه (درست) درباره‌ی ماشین دیگری مثل Φ_d، به طوری که $c < d$، که «Φ_d متوقف نمی‌شود» را می‌افزاییم. حال به وضوح ملاحظه می‌شود که $c_{\mathbf{T}_2} = c_{\mathbf{T}}$ در حالی که $c_{\mathbf{T}_1} > c_{\mathbf{T}}$. اما هیچ دلیل قانع کننده‌ای وجود ندارد که بیان کند $\mathbf{T}_1$ قوی‌تر، یا محتوای اطلاع بزرگ‌تری از $\mathbf{T}_2$ دارد. و نمی‌توان گفت پیچیدگی الگوریتمی اصول $\mathbf{T}_1$ از پیچیدگی الگوریتمی اصول $\mathbf{T}_2$ بزرگ‌تر است.

[۹] Quine

فصل ۴

ثوابت مشخصه نظریه‌های تعریف شده توسط پیچیدگی کولموگروف

۱.۴ ناتمامیت شایتین

شایتین [۴] قضیه‌ی ناتمامیت را به شکل زیر اثبات کرد: برای یک نظریه‌ی صوری، صحیح و به طور بازگشتی اصل‌پذیر $\mathbf{T}$ و یک شمارش از ماشین‌های تورینگ، کرانی مانند c موجود است به طوری که برای هر عدد n، جمله‌ی $K(n) > c$ در $\mathbf{T}$ قابل اثبات نیست. اثباتی که شایتین برای قضیه اول ناتمامیت ارایه داد مبتنی بر پارادوکس بِری می‌باشد که به ناتمامیت شایتین معروف است. شایتین برای صوری کردن پارادوکس بِری، از مفهوم پیچیدگی کولموگروف استفاده کرده است. (برای مطالعه اثبات به مرجع [۴۱] رجوع شود.) ما کوچک‌ترین چنین c ها را ثابت مشخصه شایتین نامیده و با $c_{\mathbf{T}}$ نشان می‌دهیم.

تعبیر عمومی از نتیجه شایتین این است که $c_{\mathbf{T}}$ محتوای اطلاعی یا میزان قدرت نظریه صوری $\mathbf{T}$ را اندازه‌گیری می‌کند. لامبالگن [۲۵] به این تعبیر انتقاد کرده و خاطر نشان کرد که $c_{\mathbf{T}}$ فقط و فقط توسط $\mathbf{T}$ تعیین نشده بلکه از نحوه انتخاب شمارش ماشین‌های تورینگ نیز تاثیر می‌پذیرد. راتیکاینن [۳۳] استدلال لامبالگن را قوت بخشیده و نشان داد که برای هر نظریه صوری $\mathbf{T}$، شمارشی از ماشین‌های تورینگ وجود دارد که $c_{\mathbf{T}}$ را صفر یا به طور دلخواه بزرگ می‌کند. در همان مقاله وی سعی می‌کند خاصیتی از $c_{\mathbf{T}}$ را به صورت ملموس ارایه دهد. فرض کنید $r_{\mathbf{T}}$ کوچک‌ترین کد ماشین تورینگی باشد که (روی نوار خالی) متوقف نمی‌شود، اما ما نمی‌توانیم خاصیت توقف‌ناپذیری آن را در $\mathbf{T}$ ثابت کنیم. او بیان کرد که $c_{\mathbf{T}}$ می‌تواند توسط $r_{\mathbf{T}}$ تعیین شود. ما این $r_{\mathbf{T}}$ را ثابت مشخصه راتیکاینن $\mathbf{T}$ می‌نامیم.

هدف این فصل این است که نشان دهد برخلاف ادعای راتیکاینن $c_{\mathbf{T}}$ و $r_{\mathbf{T}}$ با هم مطابقتی ندارند و همچنین نشان دهد بعضی از ویژگی‌های ریاضی $r_{\mathbf{T}}$ و $c_{\mathbf{T}}$ با هم متفاوتند. ابتدا نشان می‌دهیم به طور کلی $r_{\mathbf{T}} \leqslant c_{\mathbf{T}}$ برقرار است اما برعکس آن درست نیست. با بازچینی شمارش ماشین‌های تورینگ، می‌توانیم اختلاف بین $r_{\mathbf{T}}$ و $c_{\mathbf{T}}$ را به طور دلخواه بزرگ در نظر بگیریم. به علاوه ثابت می‌کنیم برای دو نظریه‌ی حسابی $\mathbf{T}$ و $\mathbf{S}$ با فرض وجود Π_1-جمله‌ای قابل اثبات در $\mathbf{T}$ که در $\mathbf{S}$ قابل اثبات نیست، شمارشی از ماشین‌های تورینگ موجود است که برای آن‌ها داریم $r_{\mathbf{S}} < r_{\mathbf{T}}$ و $c_{\mathbf{T}} = c_{\mathbf{S}}$.

از آنجایی که این دو ثابت مشخصه به طور اساسی اطلاعاتی را درباره‌ی ماشین‌های تورینگ (که توسط $\mathbf{T}$ داده شده‌اند) ارزیابی می‌کنند، لذا فرض می‌شود زبان $\mathbf{T}$ یک روش ثابت برای بیان خروجی‌های ماشین‌های تورینگ دارد. اما، ممکن است نظریه صوری با اصول موضوعه بسیار برای خروجی‌های ماشین‌های تورینگ، هیچ حقیقتی در مورد پیچیدگی کولموگروف بیان نکند، زیرا این دو ایده ممکن است با نمادهای مختلفی بیان شده باشند که اصول موضوعه هیچ ارتباطی بین آن دو دسته از نمادها برقرار نکند. راتیکاینن از قضیه بازگشت و صحت برای رهایی از این فرض استفاده می‌کند؛ ما نظریه‌هایمان را به نظریه‌های حساب مرتبه اول، یا به نظریه‌های صوری که در آن حساب‌های مرتبه‌ی اول می‌تواند تفسیر شود، محدود می‌کنیم و فرض کنیم که نظریه‌هایمان، نظریه صحیح حسابی و به طور بازگشتی اصل‌پذیر و توسیع $\mathbf{PA}$ باشند.

۲.۴ حسابی‌سازی محاسبه‌پذیری

قضیه ۱.۲.۴. (***قضیه باقی‌مانده چینی***[۱]). *فرض کنید که به ازای هر $i < k$، $h_i < m_i$ باشد، که درآن m_iها و h_iها اعداد طبیعی‌اند، به طوری که m_iها نسبت به هم اولند. در این صورت عدد طبیعی a موجود است به طوری که به ازای هر $i < k$، $rem(a, m_i) = h_i$ می‌باشد، که در آن $rem(a, m_i)$ نشان دهنده باقی‌مانده تقسیم a بر m_i است.*

برهان. به [۱] مراجعه شود. □

تعریف ۲.۲.۴. هر زوج مرتب (x, y) از اعداد طبیعی می‌تواند توسط

$$\langle x, y\rangle = \tfrac{1}{2}(x + y)(x + y + 1) + x$$

کدگذاری شود که آن را با $pair(x, y)$ نیز نمایش می‌دهند. همچنین چندتایی $(x_0, x_1, ..., x_n)$ از اعداد طبیعی می‌تواند توسط عدد طبیعی $\langle x_0, x_1, ..., x_n\rangle$ کدگذاری شود، که به صورت استقرایی زیر برای $n \geqslant 2$ تعریف می‌شود:

[۱] Chinese Remainder Theorem

$$.\langle x_0, x_1, ..., x_n\rangle = \langle x_0, \langle x_1, ..., x_n\rangle\rangle$$

لم ۳.۲.۴. *تابع* $pair : \mathbb{N}^2 \longrightarrow \mathbb{N}$ *دوسویی است.*

برهان. برای اثبات یک به یک بودن تابع $pair$ فرض کنید که $\langle x, y\rangle = \langle x', y'\rangle$ و $x + y = k$ و $x' + y' = k'$ باشد؛ در این صورت داریم $\frac{k(k+1)}{2} + x = \frac{k'(k'+1)}{2} + x'$. حال فرض کنید که $k \neq k'$ باشد لذا یا $k < k'$ یا $k' < k$ است؛ فرض کنیم که $k < k'$ باشد که در این صورت $k + 1 \leq k'$ خواهد بود و لذا

$$\langle x, y\rangle = \frac{k(k+1)}{2} + x \leq \frac{k(k+1)}{2} + k < \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2} \leq \frac{k'(k'+1)}{2} \leq \frac{k'(k'+1)}{2} + x' = \langle x', y'\rangle$$

که متناقض با فرض است. به همین ترتیب از $k' < k$ به تناقض می‌رسیم. پس در نتیجه از آنجایی که $\langle x, y\rangle = \langle x', y'\rangle$ داریم $k = k'$ و این یعنی $x + y = x' + y'$ پس از تساوی $\frac{(x+y)(x+y+1)}{2} + x = \frac{(x'+y')(x'+y'+1)}{2} + x'$ نتیجه می‌شود که $x = x'$ و در نتیجه $y = y'$؛ پس یک به یک بودن اثبات می‌شود. حال از آنجایی که می‌دانیم هر عدد طبیعی بین دو عدد مثلثی قرار دارد، یعنی

$$\forall z \in \mathbb{N} \quad \exists k \in \mathbb{N}; \quad t_k \leq z < t_{k+1}$$

که در آن t_k نشان دهنده‌ی kامین عدد مثلثی، $t_k = \frac{k(k+1)}{2}$ است، پس برای هر $z \in \mathbb{N}$ عدد طبیعی kای موجود است که $t_k \leq z < t_{k+1}$. قرار دهید $x = z - t_k = z - \frac{k(k+1)}{2}$ و $y = k - x$؛ حال به وضوح مشاهده می‌شود که $\langle x, y\rangle = \frac{k(k+1)}{2} + x = z$ لذا تابع $pair$ پوشاست و در نتیجه دوسویی است. □

تعریف ۴.۲.۴. (تابع β گودل[۲]). تابع $\beta : \mathbb{N}^2 \longrightarrow \mathbb{N}$ که برای هر $a = \langle x, y, n\rangle$ و $i < n$ به صورت زیر تعریف می شود تابع β گودل نامیده می‌شود:

$$\beta\,(a, i) = rem\,\big(x, y(i + 1) + 1\big)$$

[۲] Gödel's Beta Function

در حقیقت این تابع باقی مانده‌ی تقسیم x به $y(i+1)+1$ را محاسبه می‌کند. n طول a نامیده می‌شود که با $|a|$ نمایش می‌دهیم. همچنین $\beta(a,i)$ با $a[i]$ نیز نمایش داده می‌شود.

لم ۵.۲.۴. *فرض کنید $f:\mathbb{N}\longrightarrow\mathbb{N}$ یک تابع دلخواه تعریف‌پذیر در* **PA** *باشد. آنگاه*

$$\mathbf{PA}\vdash\forall n\exists a\left[\left(\forall i<n\quad\beta(a,i)=f(i)\right)\wedge|a|=n\right].$$

برهان. باید ثابت کنیم که به ازای هر $n\in\mathbb{N}$ و دنباله‌ی $f(0),f(1),...,f(n\dot{-}1)$ عدد طبیعی aای موجود است به طوری که برای هر $i<n$ داشته باشیم $\beta(a,i)=f(i)$.

قرار دهید $y=n!\prod_{i=0}^{n\dot{-}1}\left(f(i)+1\right)$ و توجه داشته باشید که تمام اعداد کمتر از n، y را عاد می‌کنند. ادعا می‌کنیم $1+y,1+2y,...,1+ny$ نسبت به هم اولند. برای اثبات ادعا، فرض کنید p عدد اولی باشد که به ازای $1\leq i<j\leq n$، داشته باشیم $p\mid yj+1$ و $p\mid yi+1$. لذا طبق خواص عاد کردن $p\mid y(j-i)$. اما p نمی‌تواند y را عاد کند زیرا در این صورت از این که $p\mid yi+1$ خواهیم داشت $p\mid 1$ که متناقض با اول بودن p می‌باشد. پس $p\mid j-i$ و این بدین معنی است که $p\leq j-i<n$، و از آنجایی که اعداد اول کمتر از n، y را عاد می‌کند داریم $p\mid y$ که یک تناقض است.

حال با توجه به ادعا و قضیه ۱.۲.۴ می‌توان گفت عدد طبیعی xای موجود است به طوری که

$$\begin{aligned}x&\equiv f(0)\quad mod(1+y)\\x&\equiv f(1)\quad mod(1+2y)\\&\vdots\\x&\equiv f(n\dot{-}1)\quad mod(1+ny)\end{aligned}$$

برای $a=\langle x,y,n\rangle$ واضح است که $\beta(a,i)=f(i)$ و $|a|=n$. □

برای هر $a_0,a_1,...,a_{n-1}\in\mathbb{N}$، عدد طبیعی a عدد دنباله‌ای برای $a_0,...,a_{n-1}$ نامیده می‌شود هرگاه برای هر عدد طبیعی $i<n$ داشته باشیم $\beta(a,i)=a_i$.

از قضیه ۲.۲.۱ نتیجه می‌شود که نظریه‌های شامل **PA**، Σ_1-جمله‌های درست در $\mathbb{N}$ را ثابت می‌کنند. همانگونه که در بخش ۲.۴.۱ بیان کردیم ماشین تورینگ M را به صورت زیر در نظر

می‌گیریم. M نواری دارد که از سمت چپ شروع می‌شود. M در یک حرکت، حالت را تغییر می‌دهد، یک نماد را روی نوار می‌نویسد، و باعث حرکت به سمت چپ یا راست می‌شود یا حرکت نمی‌کند. فرض کنیم که نمادهای نوار 0 و 1 و B باشند که B نشان دهنده‌ی نماد خالی است.

تعریف ۶.۲.۴. دو تابع جزیی f و g را تعریف شده روی $\mathbb{N}$ در نظر بگیرید؛ در این صورت $f \simeq g$ اگر و فقط اگر برای هر $x \in \mathbb{N}$ داشته باشیم $g(x) = f(x)$.

ما یک نتیجه بنیادی از نظریه‌ی بازگشت اثبات شده توسط کلینی را به کار می‌گیریم.

حقیقت ۷.۲.۴. (قضیه بازگشت کلینی[۳]). اگر f یک تابع تام محاسبه پذیر باشد، ثابتی مانند c به طور مؤثر وجود دارد به طوری که $\Phi_{f(c)} \simeq \Phi_c$.

عبارت «محاسبه‌ی $\Phi_m(0)$ به طور متعارف متوقف نمی‌شود» یا «$\Phi_m(0)\uparrow$» را می‌توان با فرمول زیر بیان کرد:

$$\forall p \left[(\Psi_0(p,m) \wedge p[0] = \langle I_M, 0, 0 \rangle) \rightarrow p \text{ متعارفاً پایان‌پذیر نیست} \right].$$

هر شمارش کارآمد از توابع محاسبه‌پذیر (یا توابع بازگشتی) می‌تواند توسط یک ماشین تورینگ جهانی نمایش داده شود [۱۴]. بنابراین، تابع دوسویی تام محاسبه‌پذیر f (f یک تابع «مترجم[۴]» است) موجود است به طوری که اگر m کد («برنامه[۵]») تابعی در آن ماشین تورینگ جهانی باشد، آنگاه تابع جزئی g کد شده با m توسط ماشین تورینگ جهانی، $g \simeq \Phi_{f(m)}$ را ارضا می‌کند. برعکس، برای هر تابع دوسویی محاسبه‌پذیر f، $\Phi_{f(m)}$ $(m = 0, 1, 2, ...)$ یک شمارش کارآمد از هر تابع محاسبه‌پذیر است. ما Φ^f_m را به جای $\Phi_{f(m)}$ می‌نویسیم. وهمچنین اگر $\Phi_{f(m)}(x) \downarrow y$ آن را به شکل $\Phi^f_m(x) \downarrow y$ نوشته و اگر $\Phi_{f(m)}(x)\uparrow$ آن را به صورت $\Phi^f_m(x)\uparrow$ می‌نویسیم. اگر ورودی 0 باشد آن را به طور صریح مشخص نخواهیم کرد؛ به جای $\Phi^f_m(0)\uparrow$، $\Phi^f_m\uparrow$ را نوشته و به جای $\Phi^f_m \downarrow y$، $\Phi^f_m \downarrow y$ را می‌نویسیم. توجه کنید که هر تابع محاسبه‌پذیر در **PA**، Σ_1-تعریف‌پذیر است [۲].

---

[۳] Kleene's Recursion Theorem

[۴] Compiler

[۵] Program

تعریف ۸.۲.۴. فرض کنید f یک تابع دوسویی Σ_1-تعریف‌پذیر در **PA** باشد. $CT(d,m)$ را فرمولی در نظر بگیرید که بیان می‌کند d کد یک ID است که پایان متعارفی از m را ارایه می‌دهد و $tval(d,x)$ فرمولی باشد که بیان می‌کند d کد یک ID است با نواری که مقدار آن توسط x نمایش داده می‌شود. ما $\Phi^f_m(x)\downarrow y$ را به جای فرمول

$$\exists p\left[\Psi_2\left(p,f\left(m\right),x\right)\wedge\exists l\left(|p|=l\wedge CT(p[l],m)\wedge tval(p[l],y)\right)\right]$$

می‌نویسیم. اگر محاسبه‌ی Φ^f_m متعارفاً پایان نپذیرد آن را با $\Phi^f_m\uparrow$ نشان می‌دهیم که معادل است با

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

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 $\Phi^f_k=n$ 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.

۳.۴ ثوابت مشخصه

تعریف ۱.۳.۴. $\mathbf{T}$ را یک سیستم صوری و توسیع **PA** در نظر بگیرید. دو ثابت مشخصه $c_{f,\mathbf{T}}$ و $r_{f,\mathbf{T}}$ را به صورت زیر تعریف می‌کنیم:

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

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

قضیه ۲.۳.۴. *برای هر سیستم صوری صحیح و به طور بازگشتی اصل‌پذیر* $\mathbf{T}$ *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 استفاده از 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 $\mathbf{T} \nvdash \Phi_c \uparrow$. □

حال نشان می‌دهیم که $r_{f,\mathbf{T}} \leq c_{f,\mathbf{T}}$.

لم ۳.۳.۴. *$\mathbf{T}$ را یک سیستم صوری و توسیع $\mathbf{PA}$ و f را یک جایگشت Σ_1-تعریف‌پذیر دلخواه در نظر بگیرید. برای هر $i < r_{f,T}$، یا $\mathbf{T} \vdash \Phi_i^f \uparrow$ یا $\mathbf{T} \vdash \Phi_i^f \downarrow$.*

برهان. چون $\mathbf{T}$ توسیع $\mathbf{PA}$ است پس تمام Σ_1-جملات درست در $\mathbb{N}$ را اثبات می‌کند، و همانطور که توضیح دادیم $\Phi_i^f \downarrow n$ توسط یک Σ_1-جمله بیان می‌شود، بنابراین اگر $\Phi_i^f \downarrow n$، آنگاه $\mathbf{T} \vdash \Phi_i^f \downarrow n$. و اگر $\Phi_i^f \uparrow$ در این صورت با توجه به تعریف ۱.۳.۴ و کمینگی $r_{f,\mathbf{T}}$، خواهیم داشت $\mathbf{T} \vdash \Phi_i^f \uparrow$. □

قضیه ۴.۳.۴. *برای هر سیستم صوری $\mathbf{T}$ که توسیع $\mathbf{PA}$ است و هر جایگشت تعریف‌پذیر f، داریم $r_{f,\mathbf{T}} \leq c_{f,\mathbf{T}}$.*

برهان. فرض (خُلف) کنید $r_{f,\mathbf{T}} > c_{f,\mathbf{T}}$ باشد. و فرض کنید $n \notin \{\Phi_0^f(0), ..., \Phi_{c_{f,\mathbf{T}}}^f(0)\}$، $i \leq c_{f,\mathbf{T}}$ بوده و $k \neq n$ باشد؛ اگر $\mathbf{T} \vdash \Phi_i^f \downarrow k$ پس $\mathbf{T} \vdash \neg(\Phi_i^f \downarrow n)$. درغیر این صورت، با توجه به این که $i < r_{f,\mathbf{T}}$ از لم ۳.۳.۴ نتیجه می‌شود که $\mathbf{T} \vdash \Phi_i^f \uparrow$ پس $\mathbf{T} \vdash \neg(\Phi_i^f \downarrow n)$. دیدیم که در هر دو حالت $\mathbf{T} \vdash \neg(\Phi_i^f \downarrow n)$ پس به ازای هر $i \leq c_{f,\mathbf{T}}$، $K^f(n) \neq i$. لذا $\mathbf{T} \vdash K^f(n) > c_{f,\mathbf{T}}$ که یک تناقض با تعریف $c_{f,\mathbf{T}}$ است. □

به هر حال، لزوماً $r_{\mathbf{T}} \geq c_{\mathbf{T}}$ برقرار نیست. در حقیقت، برای یک سیستم صوری داده شده $\mathbf{T}$ می‌توانیم ماشین‌های تورینگ را به گونه‌ای فهرست کنیم که داشته باشیم $r_{\mathbf{T}} < c_{\mathbf{T}}$.

ملاحظه ۵.۳.۴. *برای هر جایگشت تعریف‌پذیر* $\sigma : \mathbb{N} \longrightarrow \mathbb{N}$ *در* **PA**، *داریم* $\mathbf{PA} \vdash \Phi_m^{f o \sigma} \simeq \Phi_{\sigma(m)}^f$.

لم ۶.۳.۴. *فرض کنید* $f : \mathbb{N} \longrightarrow \mathbb{N}$ *یک تابع دوسویی* Σ_1*-تعریف‌پذیر در* **PA** *باشد. نگاشت* $g : \mathbb{N} \longrightarrow \mathbb{N}$، Σ_1*-تعریف‌پذیر در* **PA** *موجود است که برای هر سیستم صوری* **T** *که توسیع* **PA** *باشد داریم:*

۱. $\mathbf{T} \vdash \Phi_m^f \uparrow$ *اگر و فقط اگر* $\mathbf{T} \vdash \Phi_{g(m)}^f \uparrow$ و

۲. $\mathbf{T} \vdash \neg(\Phi_{g(m)}^f \downarrow 0)$.

برهان. ماشین تورینگی با اضافه کردن قوانین انتقال می‌سازیم که قبل از توقف روی نوار 1 بنویسد. فرض کنید m یک عدد طبیعی بوده و $M = (S_M, \Gamma, \delta_M, I_M, F_M)$ را ماشین تورینگی در نظر بگیرید که توسط $f(m)$ کدگذاری شده است. فرض کنید $M' = (S_M \cup \{q_f\}, \Gamma, \delta', I_M, \{q_f\})$ ماشین تورینگی باشد که در آن $\delta' = \delta \cup \{(q, b, q_f, 1, S) : b \in \{0, 1, B\}, q \in F_M\}$ بوده و q_f یک حالت جدید می‌باشد. فرض کنید m' کد M' و $g(m) = f^{-1}(m')$ باشد. ادعا می‌کنیم که g تابع مطلوب است.

ابتدا (۲) را نشان می‌دهیم، یعنی $\mathbf{PA} \vdash \neg(\Phi_{g(m)}^f \downarrow 0)$. درحالتی که $\Phi_{g(m)}^f \uparrow$ باشد، آنگاه $\neg(\Phi_{g(m)}^f \downarrow 0)$. در غیر اینصورت $\Phi_{g(m)}^f$ متوقف شده و برای بعضی yها خواهیم داشت $\Phi_{g(m)}^f \downarrow y$. اما با توجه به ساختار M' داریم $y \neq 0$. پس در هر حالت $\mathbf{PA} \vdash \neg(\Phi_{g(m)}^f \downarrow 0)$. حال (۱) را نشان می‌دهیم. فرض کنید $\mathbf{T} \vdash \Phi_m^f \uparrow$. پس

$$\mathbf{T} \vdash \forall p(\Psi_2(p, f(m), 0) \longrightarrow \neg\exists l(|p| = l \wedge CT(p\,[l], m) \wedge tval(p[l], y))).$$

استدلال پیش رو را می‌توان در **T** انجام داد. فرض کنید p' یک عدد طبیعی دلخواه و Σ_1-فرمول $\Psi_2(p', f(g(m), x)$ درست باشد. فرض کنید آخرین ID در p' حالت نهایی از M' را داشته باشد. آخرین ID در p' را حذف کرده و آن را p می‌نامیم. با توجه به تعریف M'، p محاسبه‌ی معتبر «$f(m)$» را نشان می‌دهد که متعارفاً پایان یافته است. بنابراین داریم $\Phi_{f(m)} \downarrow$ که یک تناقض است. درنتیجه آخرین ID در p'، حالت نهایی از M' را ندارد.

بر عکس، فرض کنید

$$\mathbf{T} \vdash \forall p'(\Psi_2(p', m', 0) \longrightarrow \neg\exists l(|p'| = l \wedge CT(p'\,[l]\,, m') \wedge tval(p'[l], y)))،$$

که در آن $m' = f(g(m))$ کد ماشین تورینگ M' توصیف شده در بالا است. فرض کنید p یک عدد طبیعی دلخواه بوده و $\Psi_2(p, f(m), x)$ برقرار باشد. اگر p محاسبه معتبری از M که متعارفاً متوقف می‌شود را نشان دهد، می‌توانیم ID از M' به p اضافه کنیم تا کدی مانند p' از محاسبه‌ی معتبر M' که متعارفاً متوقف می‌شود به دست آید. این متناقض با فرض است. بنابراین، p محاسبه‌ای معتبر از M که متعارفاً متوقف می‌شود را نشان نمی‌دهد. □

قضیه ۷.۳.۴. *فرض کنید* $\mathbf{T}$ *یک سیستم صوری و توسیع* $\mathbf{PA}$ *بوده و* $f : \mathbb{N} \longrightarrow \mathbb{N}$ *یک تابع دوسویی* Σ_1*-تعریف‌پذیر در* $\mathbf{PA}$ *باشد. بنابراین جایگشت* σ *روی* $\mathbb{N}$ *تعریف‌پذیر در* $\mathbf{PA}$ *موجود است به طوری که* $r_{f,\mathbf{T}} = r_{fo\sigma,\mathbf{T}} < c_{fo\sigma,\mathbf{T}}$.

به علاوه، اختلاف بین $r_{fo\sigma,\mathbf{T}}$ *و* $c_{fo\sigma,\mathbf{T}}$ *می‌تواند به‌طور دلخواه بسیار بزرگ باشد.*

برهان. فرض کنید n یک عدد طبیعی دلخواه باشد. نشان می‌دهیم که جایگشت σ روی $\mathbb{N}$ موجود است به طوری که $r_{f,\mathbf{T}} = r_{fo\sigma,\mathbf{T}} < c_{fo\sigma,\mathbf{T}}$ بوده و اختلاف بین $r_{fo\sigma,\mathbf{T}}$ و $c_{fo\sigma,\mathbf{T}}$ بزرگ‌تر از n است. فرض کنید $g : \mathbb{N} \longrightarrow \mathbb{N}$ تابع به دست آمده در لم ۶.۳.۴ نسبت به f باشد. و فرض کنید σ جایگشتی روی $\mathbb{N}$ باشد به طوری که برای $i \leq r_{f,\mathbf{T}} + n$ داشته باشیم $\sigma(i) = g(i)$. با توجه به لم ۳.۳.۴، برای هر $i < r_{f,\mathbf{T}}$، یا $\mathbf{T} \vdash \Phi_i^{fo\sigma} \downarrow$ یا $\mathbf{T} \vdash \Phi_i^{fo\sigma} \uparrow$. اما برای $i \leq r_{f,T} + n$، $\mathbf{T} \vdash \neg(\Phi_i^{fo\sigma} \downarrow 0)$. بنابراین $\mathbf{T} \vdash K^{fo\sigma}(0) > r_{f,\mathbf{T}} + n$. درنتیجه $r_{f,\mathbf{T}} + n < c_{fo\sigma,\mathbf{T}}$ برقرار است. □

لم ۸.۳.۴. *فرض کنید* $\psi(x)$ *یک* Δ_0*-فرمول در* $\mathcal{L}_A$ *باشد. آنگاه ماشین تورینگی باکد* m_0 *وجود دارد به طوری که*

$$\left[\mathbf{PA} \vdash \psi(x)\right] \longleftrightarrow \Phi_{m_0}(x) \downarrow 1 \quad \text{و}$$
$$\left[\mathbf{PA} \vdash \neg\psi(x)\right] \longleftrightarrow \Phi_{m_0}(x) \downarrow 0 \,.$$

برهان. $\psi(x)$ را یک Δ_0-فرمول دلخواه و ماشین تورینگ Φ_{m_0} را که در ادامه تعریف می‌شود در نظر بگیرید: Φ_{m_0} برهانی برای $\psi(x)$ و $\neg\psi(x)$ از $\mathbf{PA}$ 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 $\mathbf{PA} \vdash \psi(x)$، در این صورت با توجه به روند ساخت Φ_{m_0}، $\Phi_{m_0} \downarrow 1$؛ و اگر $\mathbf{PA} \vdash \neg\psi(x)$ آنگاه $\Phi_{m_0} \downarrow 0$. برای عکس، اگر $\Phi_{m_0} \downarrow 1$ در این صورت با توجه به توضیحات فوق، Φ_{m_0} برهانی برای $\psi(x)$ را از **PA** یافته است؛ پس $\mathbf{PA} \vdash \psi(x)$. و اگر $\Phi_{m_0} \downarrow 0$، Φ_{m_0} برهانی برای $\neg\psi(x)$ را از **PA** یافته است؛ پس $\mathbf{PA} \vdash \neg\psi(x)$. □

لم ۹.۳.۴. *فرض کنید $\psi(x)$ یک Δ_0-فرمول در $\mathcal{L}_A$ باشد. آنگاه ماشین تورینگی با کد m وجود دارد به طوری که*

$$\Big[\mathbf{PA} \vdash \forall x\psi(x)\Big] \longleftrightarrow \Phi_m \uparrow .$$

برهان. فرض کنید Φ_{m_0} ماشین تورینگی باشد که با توجه به لم ۸.۳.۴ 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:

```
while (ψ(x)) x++;
```

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 ۱۰.۳.۴. 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 ۱۱.۳.۴. برای تمام nها، پردازشی از Φ_m با ورودی 0 وجود دارد به طوری که ID نهایی $\langle I_M, bin(n), 0\rangle$ بوده و اگر $n > 0$ باشد آنگاه $\psi(n-1)$ درست است.

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 ۸.۳.۴، 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 ۸.۳.۴ 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 $\forall x \psi(x)$. □

با توجه به لم ۹.۳.۴ قضیه زیر قابل بیان است.

قضیه ۱۲.۳.۴. *فرض کنید که $\mathbf{T}$ و $\mathbf{S}$، نظریه‌های صوری صحیح، به طور بازگشتی اصل‌پذیر و توسیع $\mathbf{PA}$ باشند به طوری که $\mathbf{S} < \mathbf{T}$، آنگاه گزاره‌های زیر معادلند:*

۱. *Π_1-جمله‌ی θ موجود است به طوری که $\mathbf{T} \vdash \theta$ اما $\mathbf{S} \nvdash \theta$.*

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

برهان. فرض کنید که (۱) برقرار باشد و θ را Π_1-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 ۹.۳.۴ می‌توان نتیجه گرفت که ماشین تورینگی با کد m وجود دارد که $\mathbf{T} \vdash \Phi_m \uparrow$ و $\mathbf{S} \nvdash \Phi_m \uparrow$. بنابراین، با توجه 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 این صورت $\mathbf{T}$، Π_1-جمله‌ی $\Phi_{r_{\mathbf{S}}} \uparrow$ را اثبات می‌کند در حالی که $\mathbf{S}$ نمی‌تواند آن را اثبات کند. □

به علاوه، نشان می‌دهیم که برای دو نظریه با در نظر گرفتن یک Π_1-شکاف[۱]، شمارشی از ماشین‌های تورینگ موجود است به طوری که ثابت راتیکاینن را تغییر داده اما ثابت مشخصه شایتین را بدون تغییر نگه می‌دارد.

قضیه ۱۳.۳.۴. *فرض کنید که* $\mathbf{T}$ *و* $\mathbf{S}$*، نظریه‌های صوری صحیح، به طور بازگشتی اصل‌پذیر و توسیع* $\mathbf{PA}$ *باشند.* Π_1*-جمله‌ای قابل اثبات در* $\mathbf{T}$ *که در* $\mathbf{S}$ *قابل اثبات نیست را در نظر بگیرید. در این صورت شمارشی از ماشین‌های تورینگ وجود دارد به طوری که* $c_{\mathbf{T}} = c_{\mathbf{S}}$ *و* $r_{\mathbf{S}} < r_{\mathbf{T}}$.

برهان. با توجه به لم ۶.۳.۴ و قضیه ۱۲.۳.۴، می‌توانیم فرض کنیم که $\mathbf{S} \nvdash \Phi_m \uparrow$، $\mathbf{T} \vdash \Phi_m \uparrow$ و $\mathbf{S} \vdash \neg\Phi_m \downarrow 0$. با همان برهان قضیه ۲.۳.۴، یک c در نظر می‌گیریم که $\Phi_c \uparrow$ و $\mathbf{T} \nvdash \neg\Phi_c \downarrow n$. فرض کنید f تابعی باشد که $f(m) = 0$، $f(c) = 1$ و در غیر اینصورت $f(x) = x$ باشد. چون $\mathbf{S} \nvdash \Phi_0^f \uparrow$، پس $r_{\mathbf{S}}^f = 0$. با توجه به این که $\mathbf{T} \vdash \Phi_0^f \uparrow$ و $\mathbf{T} \nvdash \Phi_1^f \uparrow$، نتیجه می‌شود $r_{f,\mathbf{T}} = 1$. چون $\mathbf{S} \vdash K^f(0) > 0$ و برای تمام nها $\mathbf{T} \nvdash K^f(n) > 1$، پس $c_{f,\mathbf{T}} = c_{f,\mathbf{S}} = 1$ است. □

ملاحظه ۱۴.۳.۴. *در قضیه فوق، می‌توانیم* $c_{f,\mathbf{T}}$ *را همچون قضیه ۷.۳.۴ به طور دلخواه بزرگ در نظر بگیریم.*

[۱] Π_1-جمله‌ای که فقط و فقط در یکی از دو نظریه اثبات‌پذیر باشد.

فصل ۵

پیچیدگی کولموگروف و ثوابت مشخصه‌ی نظریه‌های صوری حساب

این فصل، به بحث در مورد دو ثابت مشخصه‌ی $c_{\mathbf{T}}$ و $r_{\mathbf{T}}$ پرداخته و ثابت می‌کند که $c_{\mathbf{T}}$ پیچیدگی کولموگروف $\mathbf{T}$ را نشان نمی‌دهد. در ادامه استدلال می کند که برای دو نظریه $\mathbf{S}$ و $\mathbf{T}$، همواره می‌توان ماشین تورینگ جهانی یافت که $c_{\mathbf{T}} = c_{\mathbf{S}}$. در این فصل نشان داده می‌شود که سه شرط زیر معادلند:

۱. Π_1-جمله‌ای مانند τ موجود است که در $\mathbf{T}$ قابل اثبات است ولی در $\mathbf{S}$ نیست.

۲. برای برخی از ماشین‌های تورینگ جهانی، $c_{\mathbf{S}} \neq c_{\mathbf{T}}$ برقرار است.

۳. برای برخی از ماشین‌های تورینگ جهانی، $r_{\mathbf{S}} \neq r_{\mathbf{T}}$ برقرار است.

برای این منظور ابتدا تغییراتی در ماشین‌های تورینگ داده سپس با استفاده از این تغییرات اثبات‌پذیری عدم توقف یک ماشین تورینگ را با تولیدناپذیری بعضی اعداد خاص توسط ماشین تورینگ دیگر، شرح می‌دهیم. سپس به بحث در مورد ثوابت مشخصه پرداخته و نشان می‌دهیم که با انتخاب ماشین تورینگ جهانی مناسب، مقدار $c_{\mathbf{T}}$ می‌تواند تغییر کند و به این نحو تعبیر عمومی شایتین را رد می‌کنیم. و در پایان به اثبات هدف اصلی این فصل می‌پردازیم.

۱.۵ ماشین‌های تورینگ در PA

منظور ما از یک نظریه، نظریه‌ای به طور بازگشتی اصل‌پذیر، سازگار و توسیع **PA** است. همانطور که در بخش ۲.۴.۱ بیان شد، یک شمارش از تمام ماشین‌های تورینگ مانند Φ_0 و Φ_1 و ... را با ماشین تورینگ جهانی مانند Φ نمایش می‌دهیم. فرض کنید $M(\overline{x})$ ماشین تورینگی روی ورودی $\overline{x}$ باشد؛ اگر $M(\overline{x})$ با خروجی y متوقف شود می‌نویسیم $M(\overline{x}) \downarrow y$ یا به صورت ساده‌تر می‌نویسیم $M(\overline{x}) \downarrow$؛ در غیر این صورت می‌نویسیم $M(\overline{x}) \uparrow$. ماشین تورینگ دلخواه M را در نظر بگیرید. همان طور که در تعریف ۴.۴.۱ گفتیم، مجموعه حالت‌های M را با یک مجموعه‌ی متناهی مانند S_M، حالت اولیه M را با I_M، مجموعه‌ی حالت‌های نهایی M را با F_M و مجموعه دستورات M را با δ_M نشان می‌دهیم. یک توصیف لحظه‌ای، یا به اختصار یک ID، به عنوان یک ساختار سه جزیی از محتوای نوار، حالت و موقعیت سرک M در نظر گرفته شده است. یک پردازش از M، دنباله ای متناهی از توصیف‌های لحظه‌ای است که قوانین δ_M را ارضاء می‌کند. مجموعه پردازش‌های M

روی ورودی $\overline{x}$ را با $P(M,\overline{x})$ نشان می‌دهیم. این مفاهیم را در فصل قبل در زبان **PA** فرمول‌بندی کردیم به طوری که $M\downarrow$ با یک Σ_1-جمله بیان شده بود.

لم ۱.۱.۵. *فرض کنید M و N دو ماشین تورینگ باشند. جملات زیر در* **PA** *اثبات‌پذیرند:*

۱. *اگر $\overline{x}$ دنباله‌ای از اعداد طبیعی و $p,q\in P(M,\overline{x})$ باشند آنگاه یا $p\sqsubseteq q$ یا $q\sqsubseteq p$ که در آن «$\sqsubseteq$» بیان کننده‌ی «یک قطعه‌ی ابتدایی[1] از» می‌باشد.*

۲. *اگر داشته باشیم $I_M=I_N$، $\delta_M=\delta_N$ و $S_M\cap F_N=\emptyset$، آنگاه برای هر دنباله از اعداد طبیعی مانند $\overline{x}$ خواهیم داشت $P(M,\overline{x})\subseteq P(N,\overline{x})$.*

برهان. ۱. چون $p,q\in P(M,\overline{x})$، لذا طبق تعریف $P(M,\overline{x})$، p و q پردازش‌های M با ورودی $\overline{x}$ می‌باشند. در نتیجه بنا به تعریف پردازش، $m,n\in\mathbb{N}$ موجودند به طوری که $p=(ID_0,...,ID_m)$ و $q=(ID_0,...,ID_n)$؛ در نتیجه چون $m\leq n$ یا $n\leq m$ پس به وضوح یا $p\sqsubseteq q$ یا $q\sqsubseteq p$.

۲. فرض کنید که $q\in P(M,\overline{x})$ و $q=(ID_0,ID_1,...,ID_m)$. اثبات با استقراء روی m است. اگر $m=0$ باشد در این صورت $q=(ID_0)$؛ از آنجایی که $ID_0=(I_M,t,h)$ که در آن I_M حالت اولیه، t محتوای نوار و h موقعیت سَرَک M است، و با توجه به فرض $I_M=I_N$ نتیجه می‌شود که $ID_0=(I_N,t,h)$ یک توصیف اولیه برای پردازش $q=(ID_0)$ در N است؛ لذا $q\in P(N,\overline{x})$. فرض کنید که حکم برای تمامی پردازش‌های با طول کمتر از $m+1$ برقرار باشد. نشان می‌دهیم که حکم برای پردازش‌های با طول $m+1$ نیز برقرار است. فرض کنید که q پردازشی دلخواه با طول $m+1$ از M با ورودی $\overline{x}$ باشد و $q=(ID_0,ID_1,...,ID_m)$. فرض کنید p یک بخش اولیه از q با طول m است، $p=(ID_0,ID_1,...,ID_{m-1})$. بنا به فرض استقراء $p\in P(N,\overline{x})$. فرض کنید $ID_{m-1}=(q_{m-1},t_{m-1},h_{m-1})$ در این صورت $q_{m-1}\in S_N$ و از آنجایی که $p\in P(M,\overline{x})$ پس $q_{m-1}\in S_M$. از فرض مسئله می‌دانیم که $S_M\cap F_N=\emptyset$، پس $q_{m-1}\notin F_N$. با توضیح بالا می‌توان نتیجه گرفت که ماشین تورینگ N با حالت q_{m-1} متوقف نمی‌شود و δ_N را روی (q_{m-1},t_{m-1}) اثر می‌دهد و یک ID جدید می‌سازد. ولی بنا به فرض $\delta_N=\delta_M$ لذا می‌بایست ID جدید همان ID_m متعلق به q باشد. با این توضیحات، q پردازشی از N با ورودی $\overline{x}$ است. □

[1] Initial Segment

در ادامه به ماشین‌های تورینگ بدون توقف خواهیم پرداخت و این که نظریه‌ها می‌توانند عملاً تولید نشدن بعضی از اعداد خاص توسط این ماشین‌های تورینگ را ثابت کنند. ما تغییراتی در ماشین‌های تورینگ به نحوی می‌دهیم که فرض می‌کنیم تمام نظریه‌ها تولیدناپذیری بعضی از اعداد خاص توسط این ماشین‌های تورینگ را ثابت کنند اما این تغییر اثبات‌پذیر بودن عدم توقف ماشین‌های تورینگ در **PA** را حفظ می‌کند.

تعریف ۲.۱.۵. M را یک ماشین تورینگ و ℓ را یک عدد طبیعی در نظر بگیرید.

۱. ماشین تورینگ M^ℓ را به صورت زیر تعریف می‌کنیم: حالت‌های M^ℓ را همان حالت‌های M به علاوه‌ی حالت جدید q_f در نظر بگیرید به طوری که q_f تنها حالت نهایی M^ℓ باشد. دستورات M^ℓ همان دستورات M به اضافه‌ی دستورهایی باشد که به آن فرمان می‌دهد زمانی که کنترل M^ℓ به حالتی نهایی از F_M وارد می‌شود، M^ℓ مقدار نوار را ℓ کند و با حالت q_f متوقف شود.

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

جدول ۱.۵: مربوط به تعریف ۲.۱.۵

ماشین تورینگ	م. نمادهای نوار	م. حالت‌ها	حالت اولیه	م. حالت‌های نهایی	تابع انتقال
M	Γ_M	S_M	I_M	F_M	δ_M
M^ℓ	$\Gamma_M \cup \{\ell\}$	$S_M \cup \{q_f\}$	I_M	$\{q_f\}$	δ_{M^ℓ}
$M^{(\ell)}$	Γ_M	$S_M \cup \{q_f\}$	I_M	$F_M \cup \{q_f\}$	$\delta_{M^{(\ell)}}$

در جدول فوق δ_{M^ℓ} و $\delta_{M^{(\ell)}}$ از δ_M با در نظر گرفتن شرایط خاصی که در تعریف ۲.۱.۵ آمده به دست می‌آیند و اگر آن شرایط برقرار نباشند δ_{M^ℓ} و $\delta_{M^{(\ell)}}$ با δ_M برابرند. («م.» نشان دهنده‌ی «مجموعه» می‌باشد.)

با استفاده از این بهینه‌سازی، ما می‌توانیم اثبات پذیری عدم توقف یک ماشین تورینگ را با تولید ناپذیری بعضی اعداد خاص توسط ماشین تورینگ دیگر، شرح دهیم.

لم ۳.۱.۵. *M را ماشین تورینگ بدون ورودی و ℓ را یک عدد طبیعی در نظر بگیرید. در این صورت* **PA** *اثبات می‌کند که:*

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

۲. $M^{\ell}\downarrow \longrightarrow M^{\ell}\downarrow \ell$،

۳. $M^{(\ell)} \not\downarrow \ell$،

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

برهان. ۱. می‌توانیم برهان زیر را در **PA** فرمول‌بندی کنیم. فرض کنید $M\uparrow$؛ بنابراین یک پردازش طویل مانند p از M وجود دارد. با توجه به بند دوم لم ۱.۱.۵، p پردازشی از M^{ℓ} و همین طور پردازشی از $M^{(\ell)}$ است. با توجه به بند اول لم ۱.۱.۵، اگر M^{ℓ} یا $M^{(\ell)}$ متوقف شوند آنگاه p توسیعی از یک پردازش پایان‌دار از M^{ℓ} یا $M^{(\ell)}$ می‌باشد که یک تناقض است. بنابراین $M\uparrow \longrightarrow M^{\ell}\uparrow \wedge M^{(\ell)}\uparrow$.

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'_fای پایان پذیرفته و متوقف می‌شود؛ برای ارایه‌ی پردازشی پایان‌دار از $M^{(\ell)}$، به تغییر دستورات $M^{(\ell)}$ رجوع کرده و تمام پردازش‌های پایان‌دار ممکن از $M^{(\ell)}$ که p را توسیع می‌دهند را فهرست می‌کنیم. بنابراین **PA** اثبات می‌کند که حداقل یکی از این پردازش‌های پایان‌دار توسط $M^{(\ell)}$ تحقق می‌یابد، به هر حال معلوم نمی‌کنیم کدام یک از آن پردازش‌ها محقق می‌شود. بنابراین **PA**، $M\downarrow \longrightarrow M^{\ell}\downarrow \wedge M^{(\ell)}\downarrow$ را ثابت می‌کند.

۲. فرض کنید که $M^{\ell}\downarrow$؛ بنابراین پردازشی پایان‌دار از M^{ℓ} وجود دارد. از آنجایی که تنها حالت نهایی M^{ℓ}، q_f است پس با توجه به بند اول تعریف ۲.۱.۵، این پردازش با ID نهایی در حالت نهایی q_f و خروجی ℓ پایان می‌یابد پس $M^{\ell}\downarrow \ell$.

۳. این قسمت به وضوح از بند دوم تعریف ۲.۱.۵ به دست می‌آید. زیرا اگر $M^{(\ell)}$ با حالت نهایی q'_f و خروجی ℓ متوقف شود، طبق تعریف ۲.۱.۵، ماشین تورینگ پردازش‌های خود را ادامه داده و با پردازشی نوار ارزش را $\ell + 1$ کرده و با حالت نهایی q_f متوقف می‌شود. لذا هیچ گاه $M^{(\ell)} \downarrow \ell$.

۴. فرض کنید که $x \neq \ell$ و $M \downarrow x$؛ بنابراین پردازشی پایان‌دار مانند p از M با حالت نهایی q'_fای وجود دارد. با توجه به قسمت دوم تعریف ۲.۱.۵، $M^{(\ell)}$ وارد این حالت نهایی می‌شود و چون $x \neq \ell$ هیچ کاری روی نوار انجام نداده و وارد حالت نهایی q_f شده و با همان مقدار نوار x متوقف می‌شود. پس $M^{(\ell)} \downarrow x$. برای عکس فرض کنید که $x \neq \ell$ و $M^{(\ell)} \downarrow x$. فرض (خُلف) می‌کنیم که $M \not\downarrow x$. در این صورت یا $M \uparrow$ یا yای وجود دارد که $y \neq x$ و $M \downarrow y$. حالت اول، $M \uparrow$، نمی‌تواند اتفاق بیافتد زیرا با توجه به اولین بند همین لم، می‌بایست $M^{(\ell)} \uparrow$ که متناقض با فرض است. حالت دوم، $M \downarrow y$، نیز نمی‌تواند برقرار باشد. زیرا اگر $y \neq \ell$ با توجه به روند اثبات قسمت رفت، $M^{(\ell)} \downarrow y$ که متناقض با $y \neq x$ است؛ و اگر $y = \ell$ باشد $M^{(\ell)} \downarrow \ell$ با سومین بند همین لم در تناقض است. □

در لم زیر درستی Π_1-جمله‌ها را توسط ماشین‌های تورینگ ارزیابی می‌کنیم.

لم ۴.۱.۵. *برای هر Π_1-جمله‌ی φ، ماشین تورینگ D_φ وجود دارد به طوری که* **PA**، $\varphi \longleftrightarrow D_\varphi \uparrow$ *و* $D_\varphi \downarrow 0 \longleftrightarrow \neg\varphi$ *را ثابت می‌کند.*

برهان. در لم ۸.۳.۴ نشان دادیم که می‌توانیم یک ماشین تورینگ مانند D_0 را طوری بسازیم که درستی مقادیر Δ_0-جمله‌ها را ارزیابی کند. با استفاده از ماشین تورینگ D_0، ماشین تورینگ D_1 را به صورت زیر تعریف می‌کنیم: اگر برای Δ_0-فرمولی مانند $\varphi(x)$، عدد گودل $\forall x\varphi(x)$، یعنی $\ulcorner\forall x\varphi(x)\urcorner$، 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 می‌کند. اگر D_1 مشخص کرد که برای بعضی nها $\varphi(n)$ 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 $D_1 \downarrow$. □

لم ۵.۱.۵. *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* $\mathbf{T}$ *نمی‌توانند ثابت کنند* $A_{\mathbf{S},\mathbf{T}}$ *خروجی* n *را نمی‌دهد. در نتیجه هیچ یک از* $\mathbf{S}$ *و* $\mathbf{T}$ *نمی‌توانند* $A_{\mathbf{S},\mathbf{T}} \uparrow$ *را ثابت کنند.*

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 mها، $\mathbf{S}$ 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. این متناقض با سازگاری $\mathbf{S}$ یا سازگاری $\mathbf{T}$ می‌باشد. □

۲.۵ ثوابت مشخصه

راتیکاینن [۳۳] 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 قضیه ۱.۴.۳ و بخش ۱.۵.۳ بیان کردیم. وی در این مقاله، ثابت دیگری را هم معرفی نمود که آن را با $r_{\mathbf{T}}$ نمایش داده و این ثابت را نسبت به $\mathbf{T}$ و یک ماشین تورینگ جهانی به روشی مشابه $c_{\mathbf{T}}$ تعریف نمود.

تعریف ۱.۲.۵. فرض کنید $\mathbf{T}$ یک نظریه و Φ ماشین تورینگ جهانی متناظر با شمارشی بازگشتی از تمام ماشین‌های تورینگ بدون ورودی باشد.

۱. فرض کنید x یک عدد طبیعی باشد. پیچیدگی کولموگروف x، را با $K(x)$ نمایش داده و کوچک‌ترین عدد طبیعی yای است که $\Phi_y \downarrow x$.

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

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

در قضیه ۲.۳.۴ نشان دادیم که $c_{\mathbf{T}}$ و $r_{\mathbf{T}}$ برای هر نظریه صوری $\mathbf{T}$ موجودند. در تعریف فوق برای مشخص کردن ماشین تورینگ جهانی Φ، K را با K^{Φ}، $c_{\mathbf{T}}$ را با $c^{\Phi}_{\mathbf{T}}$ و $r_{\mathbf{T}}$ را با $r^{\Phi}_{\mathbf{T}}$ نشان می‌دهیم.

گزاره ۲.۲.۵. *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 برای $i < r_{\mathbf{T}}$، هیچ یک از ماشین‌های تورینگ Φ_i، n را تولید نمی‌کنند؛ زیرا اگر فرض کنید که Φ_i متوقف می‌شود، در اینصورت جمله‌ای که بیان می‌کند Φ_i خروجی m را می‌دهد، توسط یک Σ_1-جمله بیان می‌شود و از طرفی چون $\mathbf{T}$ توسیع $\mathbf{PA}$ است لذا طبق قضیه ۲.۲.۱، $\mathbf{T}$ این Σ_1-جمله را ثابت می‌کند پس $\mathbf{T} \vdash \Phi_i \downarrow m$. طبق فرض n با خروجی‌های $\{\Phi_0, \Phi_1, ..., \Phi_{r_{\mathbf{T}}-1}\}$ برابر نیست لذا $m \neq n$؛ بنابراین $\Phi_i \not\downarrow n$ در $\mathbf{T}$ قابل اثبات است؛ حال اگر Φ_i متوقف نشود، با توجه به تعریف ۱.۲.۵ و کمینگی $r_{\mathbf{T}}$، $\Phi_i \not\downarrow n$ هم در $\mathbf{T}$ قابل اثبات است. پس در هر حالت $\mathbf{T} \vdash \Phi_i \not\downarrow n$ در نتیجه با توجه به تعریف ۱.۲.۵، $\mathbf{T}$، $r_{\mathbf{T}} - 1 < K(n)$ را ثابت می‌کند. بنابراین $r_{\mathbf{T}} - 1 < c_{\mathbf{T}}$. □

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

لم ۳.۲.۵. *فرض کنید $\mathbf{S}$ و $\mathbf{T}$ توسیع‌های $\mathbf{PA}$ باشند و همچنین Φ یک ماشین تورینگ جهانی بوده و فرض کنید τ Π_1-جمله‌ای باشد که در $\mathbf{T}$ قابل اثبات است ولی در $\mathbf{S}$ قابل اثبات نیست. در این صورت:*

۱. *اگر $\{D^0_\tau, D^{(0)}_\tau\} \in \Phi_0$، آنگاه $r_{\mathbf{S}} < r_{\mathbf{T}}$.*

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

برهان. ۱. با توجه به بند اول لم ۳.۱.۵ و لم ۴.۱.۵، $\mathbf{PA}$، $D^0_\tau \uparrow\longleftrightarrow D^{(0)} \uparrow\longleftrightarrow D_\tau \uparrow\longleftrightarrow \tau$ را اثبات می‌کند. بنابراین چون متوقف نشدن $D^{(0)}_\tau$ و D^0_τ در $\mathbf{PA}$ ثابت می‌شود پس بنا به فرض متوقف

نشدن Φ_0 نیز در **PA** ثابت می‌شود؛ از طرفی چون **S**، Π_1-جمله‌ی τ را ثابت نمی‌کند لذا ماشین تورینگ Φ_0، ماشین تورینگ با کم‌ترین اندیسی است که عدم توقف آن توسط **S** قابل اثبات نیست؛ بنابراین $r_{\mathbf{S}} = 0$ و چون **T**، Π_1-جمله‌ی τ را ثابت می‌کند لذا با توجه به توضیح ارایه شده نتیجه می‌شود که **T** متوقف شدن Φ_0 را ثابت می‌کند بنابراین $r_{\mathbf{T}} > 0$.

۲. ماشین تورینگ جهانی Φ را طوری در نظر بگیرید که $\{\Phi_0, \Phi_1\} = \{A^{(0)}_{\mathbf{S},\mathbf{T}}, D^0_\tau\}$. با برهان پیش رو در **T**، نشان می‌دهیم $c_{\mathbf{T}} > 1$. با در نظر گرفتن اثبات‌پذیری Π_1-جمله‌ی τ در **T** و از آنجایی که **T** توسیع **PA** است، طبق لم ۴.۱.۵ نتیجه می‌شود که **T** متوقف نشدن D_τ را ثابت می‌کند؛ پس بنا به بند اول لم ۳.۱.۵، متوقف نشدن D^0_τ در **T** ثابت می‌شود. بنابراین برای هر n، $\mathbf{T} \vdash D^0_\tau \not\downarrow n$. از طرف دیگر، بنا به بند سوم لم ۳.۱.۵، $\mathbf{PA} \vdash A^{(0)}_{\mathbf{S},\mathbf{T}} \not\downarrow 0$. از آنجایی که **T** توسیع **PA** است، $\mathbf{T} \vdash A^{(0)}_{\mathbf{S},\mathbf{T}} \not\downarrow 0$؛ لذا **T** ثابت می‌کند که 0 توسط $A^{(0)}_{\mathbf{S},\mathbf{T}}$ و D^0_τ تولید نمی‌شود. پس با توجه به فرض که $\{\Phi_0, \Phi_1\} = \{A^{(0)}_{\mathbf{S},\mathbf{T}}, D^0_\tau\}$ و تعریف ۱.۲.۵، $\mathbf{T} \vdash 1 < K(0)$ در نتیجه $c_{\mathbf{T}} > 1$. حال ثابت می‌کنیم که $c_{\mathbf{S}} \leq 1$. فرض (خُلف) می‌کنیم که $c_{\mathbf{S}} > 1$؛ با توجه به تعریف ۵. ۱.۲، عدد طبیعی مانند n وجود دارد به طوری که $\mathbf{S} \vdash \Phi_0 \not\downarrow n$ و $\mathbf{S} \vdash \Phi_1 \not\downarrow n$ پس بنا به فرض که $\{\Phi_0, \Phi_1\} = \{A^{(0)}_{\mathbf{S},\mathbf{T}}, D^0_\tau\}$، $\mathbf{S} \vdash D^0_\tau \not\downarrow n$ و $\mathbf{S} \vdash A^{(0)}_{\mathbf{S},\mathbf{T}} \not\downarrow n$. اگر $n \neq 0$، با توجه به بند چهارم لم ۳.۱.۵ و اینکه $\mathbf{S} \vdash A^{(0)}_{\mathbf{S},\mathbf{T}} \not\downarrow n$، نتیجه می‌شود که $\mathbf{S} \vdash A_{\mathbf{S},\mathbf{T}} \not\downarrow n$ در حالی که این متناقض با روند ساخت $A_{\mathbf{S},\mathbf{T}}$ در لم ۵.۱.۵ است. حال فرض کنید که $n = 0$. در این صورت با توجه به بند دوم لم ۳.۱.۵، $\mathbf{S} \vdash D^0_\tau \not\downarrow n$ ایجاب می‌کند که $\mathbf{S} \vdash D^0_\tau \uparrow$؛ بند اول همان لم نتیجه می‌دهد که $\mathbf{S} \vdash D_\tau \uparrow$. حال از اینکه $\mathbf{S} \vdash D_\tau \uparrow$ و با استفاده از لم ۴.۱.۵ نتیجه می‌شود که $\mathbf{S} \vdash \tau$ که متناقض با فرض اثبات‌ناپذیری τ در **S** است. پس در هر حالت $c_{\mathbf{S}} \leq 1$. بنابراین $c_{\mathbf{S}} < c_{\mathbf{T}}$. □

در قضیه ۱۲.۳.۴ ثابت کردیم که برای برخی از ماشین‌های تورینگ جهانی $r_{\mathbf{S}} < r_{\mathbf{T}}$ اگر و فقط اگر Π_1-جمله‌ی قابل اثبات در **T** موجود باشد که در **S** قابل اثبات نیست که این نیز به عنوان نتیجه‌ای از قضیه زیر به دست می‌آید.

قضیه ۴.۲.۵. *S و T را توسیع* **PA** *در نظر بگیرید. گزاره‌های زیر معادلند:*

۱. *Π_1-جمله‌ای مانند τ وجود دارد که در* **T** *قابل اثبات است ولی در* **S** *نیست.*

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

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

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

برهان. فرض کنید که (۱) برقرار باشد. ماشین تورینگ جهانی Φ را طوری در نظر بگیرید که $(\Phi_0, \Phi_1) = (A^{(0)}_{\mathbf{S},\mathbf{T}}, D^0_\tau)$. با توجه به بند دو لم ۳.۲.۵، $c_{\mathbf{S}} < c_{\mathbf{T}}$. از طرفی چون هیچ کدام از $\mathbf{S}$ و $\mathbf{T}$، $\uparrow A^{(0)}_{\mathbf{S},\mathbf{T}}$ را اثبات نمی‌کنند لذا بند اول لم ۳.۱.۵، $r_{\mathbf{S}} = r_{\mathbf{T}} = 0$ را در پی دارد. در نتیجه (۲) درست است. با در نظر گرفتن (۲) و بند اول لم ۳.۲.۵ و این که $(\Phi_0, \Phi_1) = (D^0_\tau, A^{(0)}_{\mathbf{S},\mathbf{T}})$ (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 $^{(0)}$ افزایش 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 $i < c_{\mathbf{T}}$، $\mathbf{S}$، $\Phi_i \not\downarrow n$ را ثابت نمی‌کند که در آن $\Phi_i \not\downarrow n$ توسط یک Π_1-جمله بیان شده است. اگر $r_{\mathbf{S}} < r_{\mathbf{T}}$ آنگاه $\mathbf{T}$، Π_1-جمله‌ی $\Phi_{r_{\mathbf{S}}} \uparrow$ را اثبات می‌کند در حالی که $\mathbf{S}$ نمی‌تواند آن را اثبات کند. □

ملاحظه ۵.۲.۵. *نیازی نیست که فرض کنیم* $\mathbf{T}$ *نظریه‌ی قوی‌تری نسبت به* $\mathbf{S}$ *است تا* $c_{\mathbf{S}} < c_{\mathbf{T}}$ *یا* $r_{\mathbf{S}} < r_{\mathbf{T}}$ *را ثابت کنیم. از طرف دیگر، اختلاف بین* $c_{\mathbf{T}}$ *و* $r_{\mathbf{T}}$ *نسبت به یک ماشین تورینگ جهانی کران‌دار نیست.*

گزاره ۶.۲.۵. *برای هر ماشین تورینگ جهانی بدون ورودی* Φ *و هر عدد طبیعی دلخواه* n*، ماشین تورینگ جهانی* Ψ *موجود است به طوری که* $K^\Phi = K^\Psi$*،* $r^\Phi_{\mathbf{T}} = r^\Psi_{\mathbf{T}}$ *و* $r^\Psi_{\mathbf{T}} + n < c^\Psi_{\mathbf{T}}$.

برهان. برای هر $l \leq r^\Phi_{\mathbf{T}} + n + 1$، یک ماشین تورینگ جهانی تعریف می‌کنیم به طوری که برای هر $i \leq r^\Phi_{\mathbf{T}} + n$، هیچ jای موجود نباشد که $\Psi_{li} = \Psi^{(l)}_{lj}$. $\mathbf{T}$ ثابت می‌کند که l نمی‌تواند توسط هیچ یک از Ψ_{l0} و Ψ_{l1} و ... و $\Psi_{lr^\Phi_{\mathbf{T}}+n}$ تولید شده باشد و در نتیجه داریم $r^\Phi_{\mathbf{T}} + n < K^{\psi_l}(l)$. از طرف دیگر، چون $\mathbf{T}$ برای تمام $i \leq r^\Phi_{\mathbf{T}} + n$، $\Phi_i \uparrow \longleftrightarrow \Psi_{li} \uparrow$ را ثابت می‌کند، داریم $r^\Phi_{\mathbf{T}} = r^{\Psi_l}_{\mathbf{T}}$. حداقل یکی از این lها همواره $K^\Phi = K^{\Psi_l}$ را ارضا می‌کند. N را مجموعه‌ی خروجی‌های Ψ_{l0} و Ψ_{l1} و ... و

$\Psi_{lr^{\Phi}_{\mathbf{T}}+n}$ در نظر بگیرید. چون N شامل حداکثر $r^{\Phi}_{\mathbf{T}}+n+1$ عضو است، می‌توانیم $l_0 \leq r^{\Phi}_{\mathbf{T}}+n+1$ در نظر بگیریم که در N ظاهر نمی‌شود. پس داریم $r^{\Phi}_{\mathbf{T}}+n < K^{\Phi}(l_0)$ و در نتیجه $K^{\Phi} = K^{\Psi_{l_0}}$ برقرار است. □

مراجع

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

[2] G. Boolos, J. Burgess, R. Jeffrey, **Computability and Logic**, *Cambridge University Press, Cambridge, 5th ed. (2007).*

[3] G. CHOQUET, *Repartition des nombres $k(3/2)^n$ mod 1; mesures et ensembles associes,* **Comptes Rendus des Sances de l'Academie des Sciences, Series A-B**, *vol. 290 (1980). pp. A575-A580.*

[4] G. J. Chaitin, **Information-Theoretic Limitations of Formal Systems**, *Journal of the ACM 21 (1974), pp. 403–424.*

[5] G. J. Chaitin, **A Theory of Program Size Formally Identical to Information Theory,** *Journal of the Association for Computing Machinery, vol. 2^2 (1975), pp. 329-340.*

[6] G. J. Chaitin, **Algorithmic Information Theory,** *IBM Journal of Research and Development, vol. 21 (1977), pp. 350-359, 496.*

[7] G. J. Chaitin, **Göbdel's Theorem and Information,** *International Journal of Theoretical Physics, vol. 21 (1982), pp. 941-954.*

[8] G. J. Chaitin, **Incompleteness Theorems for Random Reals**, *Advances in Applied Mathematics, vol.8(1987), pp. 119-146.*

[9] G. J. Chaitin, **Algorithmic Information Theory**, *Cambridge Tracts in Computer Science, vol. 1, Cambridge University Press, Cambridge, (1987).*

[10] F. M. DEKKING, *Regularity and irregularity of sequences generated by automata,* **Seminaire de theorie des nombres, 1979-1980**, *Universite de Bordeaux I, Talence, (1980), Expose 9.*

[11] M. Davis, *What is a Computation?* **Mathematics Today**, *(L. A. Steen, editor), Springer-verlag, Berlin, (1978), pp. 241-267.*

[12] M. DAVIS, Y. MATIJASEVI and J. ROBINSON, *Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution,* **Mathematical Developments Arising from Hilbert Problems**, *(F. E. Browder, editor), American Mathematical Society, Providence, Rhode Island, (1976), pp. 323-378.*

[13] H. B. Enderton, **A Mathematical Introduction to Logic**, *Academic Press, Second edition, (2001).*

[14] A. G. Hamilton, **Logic for Mathematicians**, *Cambridge University Press, (1988).*

[15] P. G. Hinman, **Fundamentals of Mathematical Logic**, *A K Peters, Ltd, (2005).*

[16] S. Ibuka, & M. Kikuchi, & H. Kikyo, **On Characteristic Constants Defined by Kolmogorov Complexity**, *in: M. Hodges, & R. de Queiroz, (eds.) Logic, Language, Information and Computation, 15th International Workshop, WoLLIC 2008, Edinburgh, UK, July 1–4, 2008, Lecture Notes in Artificial Intelligence, Vol. 5110 (Springer-Verlag, 2008), pp. 218–225.*

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

[18] A. N. Kolomogorov, **On Tables of Random Numbers** , *Sankhya-Series A, vol. 25(1963), pp.369-376.*

[19] A. N. Kolomogorov, **Three Approaches to the Definition of the Concept of "Amount of Information"** , *Selected translations in mathematical statistics and probability, vol. 7, American Mathematical Society, Providence, Rhode Island, (1968), pp. 293-302.*

[20] A. N. Kolomogorov, **The Logical Basis for Information Theory and Probability Theory** , *IEEE Transactions on Information Theory, vol. IT-14 (1968), pp. 662-664.*

[21] A. N. Kolomogorov, **Combinatorial Basis for Information Theory and Probability Theory** , *Russian Mathematical Surveys, vol. 38 (1983), no. 4, pp. 29-40.*

[22] A. N. Kolomogorov, **On Logical Foundations of Probability Theory** , *Probability theory and mathematical statistics (proceedings of the fourth USSR-Japan symposium, Toilisi, 1982; K. 1t6 and J. V. Prokhorov, editors), Lecture Notes in Mathematics, vol. 1021, Springer-Verlag, Berlin, 1984, pp. 1-5.*

[23] G. Kreisel & A. Levy, *Reflection Principles and Their Use for Establishing the Complexity of axiomatic systems,* **Zeitschrift für Mathematische Logik und Grundlagen der Mathematik**, *vol. 14 (1968), pp.97-142.*

[24] KEN-I Ko, *On the notion of infinite pseudorandom sequences,***Theoretical Computer Science**, *vol. 48 (1986), pp. 9-33.*

[25] M. van Lambalgen, **Algorithmic Information Theory**, *Journal of Symbolic Logic 54 (1989), pp. 1389–1400.*

[26] M. van Lambalgen, **Random Sequences**, *Ph.D. thesis, Department of Mathematics, University of Amsterdam, Amsterdam, (1987).*

[27] M. Li, & P. Vitanyi, **An Introduction to Kolmogorov Complexity and Its Applications**, *Springer, 3rd ed. (2008).*

[28] P. Linz, **An Introduction to Formal Languages and Automata**, *Jones & Bartlett Learning, 5th ed. (2011).*

[29] D. Marker, **Model theory: an introduction**, *Springer, (2002).*

[30] P. Martin-Löf, *The Definition of random Sequences,* **Information and Control,** *vol. 9 (1966), pp. 602-619.*

[31] P. Martin-Löf, *a)* **Algorithmen und Zufällige Folgen**, *lecture notes, University of Erlangen, Erlangen, (1966).*

b) *Complexity oscillations in infiniteb inary sequences,* **Zeitschrift fur Wahrscheinlichkeitstheorie und Verwandte Gebiete**, *vol. 19 (1971), pp. 225-230.*

[32] H. Rogers, **Theory of Recursive Functions and Effective Computability**, *McGraw-Hill, New York, (1967).*

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

[34] W. Rautenberg, **A Concise Introduction to Mathematical Logic**, *Springer, 3rd ed. (2010).*

[35] *C. P. Schnorr,* **Zufälligkeit und Wahrcheinlichkeit** , *Lecture Notes in Mathematics, vol. 218, Springer-Verlag, Berlin, (1971).*

[36] C. Smorynski, *The Incompleteness Teorems,* **Handbook of Mathematical Logic,** *(J. Barwise, editor), Noth-Holland, Amsterdam, (1977), pp. 821-865.*

[37] P. Smith, **An Introduction to Gödel's Theorems**, *Cambridge University Press, Second edition, (2013).*

[38] R. I. Soare, **Recursively Enumerable Sets and Degrees**, *Springer-Verlag, Berlin, (1986).*

[39] R.M. Solovay, **A Version of Ω for Which ZFC Can Not Predict A Single Bit**, *in: Calude, C. Păun, G. (eds.) Finite Versus Infinite: Contributions to an Eternal Dilemma (2000), Springer, pp. 323-334.*

[40] T. Tymoczko (editor), **New Directions in Philosophy of Mathematics**, *Birkhäuser, Boston, Massachusetts, (1986).*

[۴۱] پ. قائمی، **پارادوکس آزمون ناگهانی و قضیه دوم ناتمامیت**، *پایان‌نامه کارشناسی ارشد، دانشکده ریاضی، دانشگاه تبریز*، (۱۳۹۳).

واژه‌نامه فارسی به انگلیسی

استقراء ..... Induction
اصل‌پذیر ..... Axiomatizable
الحاق ..... Concatenation
الفبا ..... Alphabet
انتقال ..... Transition
بازگشتی ..... Recursive
برنامه ..... Program
برهان ..... Proof
پیچیدگی کولموگروف ..... Kolmogorov Complexity
پیکربندی ..... Configuration
تابع بازگشتی ..... Recursive Function
تابع β گودل ..... Gödel's Beta Function
تابع دوتایی ..... Binary Function
تعریف‌پذیری ..... Definability
تك موضعی ..... Unary
تناظر یك به یك و پوشا ..... Bijection
توسیع ..... Extending
توصیف لحظه‌ای ..... Instantaneous Descriptions
ثابت مشخصه ..... Characteristic Constant
جمله ..... Sentence
حساب ..... Arithmetic
حساب پئانو ..... Peano Arithmetic

دنباله ..... Sequence
رشته ..... String
زبان ..... Language
زبان صوری ..... Formal Language
سازگار ..... Consistent
سَرَک ..... Head
سور ..... Quantifier
شمارش ..... Enumeration
شمارش‌پذیر ..... Countable
شمارش‌پذیر کارآمد ..... Effectively Countable
عملگر ..... Operator
قضیه ..... Theorem
قضیه بازگشت کلینی ..... Kleene's Recursion Theorem
ماشین تورینگ ..... Turing Machine
ماشین تورینگ جهانی ..... Universal Turing Machine
مترجم ..... Compiler
محاسبه‌پذیر ..... Computable
مقدماتی ..... Elementary
منطق مرتبه اول ..... First-Order Logic
ناسازگار ..... Inconsistent
نتیجه ..... Conclusion
نظریه ..... Theory
نظریه صحیح ..... Sound
نوار ..... Tape

واژه‌نامه انگلیسی به فارسی

الفبا ..... Alphabet
حساب ..... Arithmetic
اصل‌پذیر ..... Axiomatizable
تناظر یك به یك و پوشا ..... Bijection
تابع دوتایی ..... Binary Function
ثابت مشخصه ..... Characteristic Constant
محاسبه‌پذیر ..... Computable
سازگار ..... Consistent
شمارش‌پذیر ..... Countable
مترجم ..... Compiler
الحاق ..... Concatenation
نتیجه ..... Conclusion
پیکربندی ..... Configuration
تعریف‌پذیری ..... Definability
شمارش‌پذیر کارآمد ..... Effectively Countable
مقدماتی ..... Elementary
شمارش ..... Enumeration
توسیع ..... Extending
تابع β گودل ..... Gödel's Beta Function
سَرَک ..... Head
منطق مرتبه اول ..... First-Order Logic
زبان صوری ..... Formal Language

ناتمامیت ..... Incompleteness
ناسازگار ..... Inconsistent
استقراء ..... Induction
توصیف لحظه‌ای ..... Instantaneous Descriptions
قضیه بازگشت کلینی ..... Kleene's Recursion Theorem
پیچیدگی کولموگروف ..... Kolmogorov Complexity
زبان ..... Language
عملگر ..... Operator
حساب پئانو ..... Peano Arithmetic
برنامه ..... Program
برهان ..... Proof
سور ..... Quantifier
بازگشتی ..... Recursive
تابع بازگشتی ..... Recursive Function
جمله ..... Sentence
دنباله ..... Sequence
نظریه صحیح ..... Sound
رشته ..... String
نوار ..... Tape
قضیه ..... Theorem
نظریه ..... Theory
انتقال ..... Transition
ماشین تورینگ ..... Turing Machine
ماشین تورینگ جهانی ..... Universal Turing Machine

نمایه

Surname: Ghanizadeh zare **Name:** Sajad

Title: Kolmogorov Complexity And Characteristic Constants Of Formal Theories Of Arithmetic

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:** 96

Keywords: Kolmogorov complexity, Characteristic constant.

Abstract

Two constants $c_{\mathbf{T}}$ and $r_{\mathbf{T}}$, introduced by Chaitin and Raatikainen respectively and defined for each recursively axiomatizable consistent theory $\mathbf{T}$ and universal Turing machine, used to determine Kolmogorov complexity, are investigate this theory. Raatikainen argued that $c_{\mathbf{T}}$ does not represent the complexity of $\mathbf{T}$ and found that for two theories $\mathbf{S}$ and $\mathbf{T}$, one can always find a universal Turing machine such that $c_{\mathbf{S}} = c_{\mathbf{T}}$. In this thesis, it is shown that the following three conditions are equivalent:

1. There is a Π_1-sentence τ which is provable in $\mathbf{T}$ but not in $\mathbf{S}$,
2. $c_{\mathbf{T}} \neq c_{\mathbf{S}}$ for some universal Turing machine, and
3. $r_{\mathbf{T}} \neq r_{\mathbf{S}}$ for some universal Turing machine.

Moreover it is shown that $r_{\mathbf{T}}$ does not necessarily coincide with $c_{\mathbf{T}}$; for two arithmetical theories $\mathbf{T}$ and $\mathbf{S}$ with a Π_1-sentence provable in $\mathbf{T}$ but not in $\mathbf{S}$, there is an enumeration of the Turing machines such that $r_{\mathbf{S}} < r_{\mathbf{T}}$ and $c_{\mathbf{S}} = c_{\mathbf{T}}$.

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 (MATHEMATICAL LOGIC)

Kolmogorov Complexity And Characteristic Constants Of Formal Theories Of Arithmetic

Supervisor

Saeed Salehi

Advisor

Hazhir Homei

by

Sajad Ghanizadeh zare

2015