。

حساب مرتبهٔ اول پئانو و زیر نظریه‌های آن همراه با چند مسئلهٔ مرتبط در نظریهٔ پیچیدگی

مرتضی منیری

دانشگاه شهید بهشتی و مرکز تحقیقات فیزیک نظری و ریاضیات

ezmoniri@ipm.ir

چکیده:

در این مقاله مروری بر نظریه های مرتبه اول حساب خواهیم داشت. همچنین، اشاره خواهیم کرد که زیر نظریه های ضعیف حساب ارتباط‌های اساسی با نظریهٔ پیچیدگی محاسبه دارند. در انتها اشاره‌ای به نظریه‌های مرتبه اول شهودی حساب خواهیم کرد.

یکی از نخستین قسمتهایی از ریاضیات که منطق‌دانان به مطالعهٔ آن پرداختند نظریهٔ اعداد طبیعی بود. در واقع مطالعهٔ خواص اعداد طبیعی (و البته نظریهٔ مجموعه‌ها) انگیزهٔ اصلی بنیان‌گذاران منطق ریاضی در اواخر قرن نوزدهم و اوایل قرن بیستم بود. دلیل این امر اهمیتی بود که آنان برای این شاخه‌ها به‌عنوان پایه‌هایی برای کل ریاضیات قایل بودند.

پئانو[۱]، ریاضی‌دان و منطق‌دان ایتالیایی، اصول موضوع معروف خود برای حساب را در سال ۱۸۸۹ میلادی معرفی کرد. این اصول، به تعبیر ما، مرتبهٔ دوم بودند زیرا به اعداد و همچنین مجموعه‌های شامل اعداد مرتبط بودند. در حال حاضر، منظور از حساب پئانو (PA)، نظیر مرتبهٔ اول اصول مطرح شده به‌وسیلهٔ پئانو است.

[۱] Peano

۱. حساب (مرتبهٔ اول) پئانو

در این قسمت به معرفی حساب پئانو در دستگاه منطق محمولات مرتبهٔ اول می پردازیم. یک زبان (مرتبهٔ اول) مناسب برای مطالعهٔ PA، $L = \{۰, ۱, +, \cdot, <\}$ است (در واقع L مجموعهٔ نمادهای ثابت، تابعی و محمولی زبان مورد نظر است). DOR^+ مجموعهٔ اصول موضوع قسمتهای مثبت حلقه‌های جابجایی و یکدار و به‌طور گسسته مرتب در زبان فوق است. در واقع DOR^+ چیزی نیست جز همان مجموعهٔ خواص معمولی جمع و ضرب و ترتیب اعداد طبیعی. برای مثال اصل $\forall x, y\, (x + y = y + x)$ جابجایی بودن جمع و اصل $\forall x, y\, (x < y \,\vee\, x = y \,\vee\, y < x)$ خطی بودن ترتیب را بیان می‌کند. DOR^+ را با PA^- نیز نشان می‌دهند.

برای بیان اصل استقراء، نیاز به کمی تأمل است. این اصل به‌صورت غیر صوری به شکل زیر بیان شده است:

"فرض کنید $A \subseteq \mathbb{N}$. ضمناً فرض کنید $۰ \in A$ و به‌ازای هر عدد طبیعی n، اگر $n \in A$ آن‌گاه $n + ۱ \in A$. در این‌صورت $A = \mathbb{N}$"

اصل فوق قابل بیان در منطق مرتبهٔ اول نیست، زیرا (تلویحاً) شامل سوری عمومی روی مجموعه‌هاست. نظیر مرتبه اول این اصل شکل زیر را خواهد داشت:

$$I_x\varphi :\ [\varphi(۰) \ \wedge\ \forall x\ (\varphi(x) \longrightarrow \varphi(x + ۱))] \longrightarrow\ \forall x\ \varphi(x)$$

به‌ازای هر فرمول φ، شامل متغیر آزاد x (و متغیرهای آزاد احتمالی دیگر).

در واقع ما با یک طرح اصل موضوعی مواجه هستیم که شامل تعدادی نامتناهی اصل است. اما این مجموعهٔ نامتناهی از اصول، قدرتی بسیار کمتر از اصل غیر صوری استقراً دارد؛ توجه کنید که مجموعهٔ زیر مجموعه‌های $\mathbb{N}$ ناشماراست ولی مجموعهٔ همهٔ فرمولها در زبان L، شمارا است.

مجموعهٔ اصول مرتبهٔ اول مطرح شدهٔ فوق همان حساب مرتبهٔ اول پئانو(PA) است:

$$PA = DOR^+ \cup \text{استقراء}$$

PA فرمولی چون φ را ثابت می‌کند، $\mathrm{PA} \vdash \varphi$، هرگاه اصول فوق در دستگاه منطق محمولات مرتبهٔ اول φ را ثابت کند. همین ضعف PA نسبت به دستگاه غیر صوری حساب است که باعث می‌شود اثبات‌های معمولی برای نشان دادن یکتایی (با تقریب یکریختی) مدل‌های دستگاه اخیر، در مورد PA کار نکنند.

۲. وجود مدل‌های نااستانده برای حساب

مدل استانده برای PA، مجموعهٔ اعداد طبیعی با جمع و ضرب و ترتیب معمولی است: $\langle \mathbb{N}, ۰, ۱, +, \cdot, < \rangle$. از این‌جا به بعد، مدل‌ها را با مجموعه‌های زمینهٔ آن‌ها نشان می‌دهیم. دو مدل M و M' از PA را یکریخت گوییم هرگاه تابعی یک‌به‌یک و پوشا چون $f : M \longrightarrow M'$ موجود باشد به طوری‌که $f(۰_M) = ۰_{M'}$، $f(۱_M) = ۱_{M'}$ و f، جمع و ضرب و ترتیب را حفظ کند.

اگر M و M' یکریخت باشند آن‌گاه به‌ازای هر فرمول $\varphi(\vec{x})$ در زبان L و هر $\vec{a} \in M^n$ ، $M \models \varphi(\vec{a})$ (M مدلی است برای جملهٔ $\varphi(\vec{a})$) اگر و تنها اگر $M' \models \varphi(f(\vec{a}))$. در اینجا منظور از $\vec{x}$ دنبالهٔ $x_۱, \ldots, x_n$ است.

هدف اولیه برای معرفی PA، آن بود که مجموعهٔ جمله‌های درست در مورد $\mathbb{N}$ ، اصطلاحاً $\mathrm{Th}(\mathbb{N})$ ، را به‌طور یکتا مشخص کند، اما به‌زودی معلوم شد که این‌کار ممکن نیست. PA دارای مدل‌های نااستانده است، یعنی مدل‌هایی که با $\mathbb{N}$ یکریخت نیستند. این مطلب را می‌توان به‌عنوان نتیجه‌ای از یکی از قضیه‌های اساسی منطق ریاضی، یعنی قضیهٔ لوونهایم—اسکولم به‌دست آورد. بنابراین قضیه، اگر نظریه‌ای در یک زبان متناهی دارای مدلی شمارای نامتناهی باشد، آن‌گاه دارای مدل‌هایی از هر عدد اصلی نامتناهی دلخواه خواهد بود. مدل‌های با عددهای اصلی متفاوت هرگز نمی‌توانند یکریخت باشند. نتایج قوی‌تری نیز در این زمینه در دست است. مثلاً می‌توان نشان داد که مجموعهٔ مدل‌های شمارای غیر یکریخت PA، ناشماراست.

روشن است که نتیجهٔ فوق (در مورد یکتا نبودن مدل‌های PA) را می‌توان در مورد هر مجموعهٔ دیگر از اصول موضوع برای حساب، به‌جای PA، نیز به‌دست آورد.

PA دستگاهی است طبیعی و زیبا و وجود مدل‌های به اندازهٔ کافی زیاد نااستانده برای آن موجب خوشحالی است، زیرا باعث باز شدن یک مسیر تحقیقاتی وسیع برای منطق‌دانان شده است که همان مطالعهٔ این مدل‌ها است. مرجع [K2] در این مورد بسیار خواندنی است. در پایین به چند تا از مهمترین خواص مدل‌های PA اشاره خواهد شد ولی قبل از آن قضیه‌های بسیار معروف ناتمامیت گدل [۲] را مرور می‌کنیم.

۳. قضیه‌های ناتمامیت گدل

آیا PA توانایی اثبات همهٔ جملات حسابی درست (در مدل $\mathbb{N}$) را دارد؟
معلوم شده است که PA قدرت زیادی دارد و اثبات‌های ارائه شده برای تمامی قضیه‌های نظریهٔ مقدماتی اعداد را می‌توان در PA صوری کرد. البته این گونه صوری‌سازی‌ها معمولاً پردردسر و دارای جزئیات زیاد است. به‌عنوان مثال، می‌توانید یک اثبات صوری از نامتناهی بودن مجموعهٔ اعداد اول را در [K۲, ۵.۳] ببینید: $\mathrm{PA} \vdash \forall x\ \exists y\ (y > x\ \wedge\ \mathrm{prime}(y))$ جایی‌که

$$\mathrm{prime}(y) \longleftrightarrow\ (y \geqslant ۲\ \wedge\ \forall z, w\ (y|zw \longrightarrow (y|z\ \vee y|w)))$$

و

$$x|y \longleftrightarrow\ (\exists z \leqslant y\ (xz = y)\ \wedge\ x \neq ۰)$$

در هر حال، قضیهٔ اول ناتمامیت گدل بیان این مطلب است که با فرض سازگاری PA جواب سؤال فوق منفی است، یعنی جمله‌ای در زبان حساب چون φ موجود است که درست است ولی PA توانایی اثبات آن‌را ندارد [۳]. قضیهٔ دوم ناتمامیت گدل مثال مشخصی از یک

[۲] Gödel

[۳] واضح است گه بنابر قضیهٔ گدل $\mathrm{PA} \nvdash \varphi$ و $\mathrm{PA} \nvdash \neg\varphi$. وجود φ با چنین خاصیتی را ناتمامیت PA می نامند. کلمهٔ تمامیت در منطق ریاضی به معنای دیگری نیز به کار می‌رود. اگر T یک نظریهٔ مرتبهٔ اول باشد آن‌گاه تمامیت T می‌تواند به این معنی نیز باشد که اگر جمله‌ای چون ψ در هر مدل از T درست بود آن‌گاه $T \vdash \psi$. به این مفهوم هر نظریهٔ مرتبهٔ اول (من جمله PA) تمام است. این مطلب همان قضیهٔ تمامیت (قوی) منطق معمولات مرتبهٔ اول است. جالب است بدانید که قضیهٔ تمامیت نیز اول بار بوسیلهٔ گدل ثابت شده است.

چنین φ ای را عرضه می‌کند، یعنی $\mathrm{Con(PA)}$. $\mathrm{Con(PA)}$ جمله‌ای است در زبان حساب که از طریق کد کردن مفاهیم فرمول خوش ساخت، دنبالهٔ متناهی از فرمول‌های خوش ساخت، اثبات و در نهایت مفهوم اثبات پذیری در PA، به‌دست آمده است:

$$\mathrm{prov}(x,y) \longleftrightarrow \text{“ } x \text{ کد اثباتی برای فرمول با کد } y \text{ است”}$$

$$\mathrm{Con\,PA} \longleftrightarrow \neg\,\exists x\,\mathrm{prov}\,(x, \overline{\circ = ۱})$$

جائیکه $\overline{\circ = ۱}$ کد فرمول $۱ = \circ$ است.

در واقع گدل نشان داد که دو قضیهٔ فوق در مورد هر تئوری سازگار شامل PA که مجموعهٔ اصول موضوعهٔ آن بازگشتی (یعنی به صورت الگوریتمیک قابل تمیز) باشد، برقرار است. توجه کنید که یک نتیجهٔ بلافاصلهٔ این قضایا این است که $\mathrm{Th}(\mathbb{N})$ به طور بازگشتی اصل پذیر نیست، در حالت خاص، خود $\mathrm{Th}(\mathbb{N})$ یک مجموعهٔ بازگشتی نیست، هیچ روش مکانیکی یا برنامه‌ای کامپیوتری برای تشخیص درستی‌های $\mathbb{N}$ موجود نیست. از طرف دیگر بنا به قضیه‌های گدل، $\mathrm{PA} + \mathrm{Con(PA)}$ و $\mathrm{PA} + \neg\,\mathrm{Con(PA)}$ سازگارند و بنابراین مدل دارند. مدل‌های این دو نظریه، مدل‌های متفاوتی از PA را به‌دست می‌دهند.

هر چند که جملهٔ $\mathrm{Con(PA)}$ از دید منطق ریاضی دارای اهمیت ذاتی است، ولی ممکن است برای ریاضیدانان، به طور اعم، چندان حائز اهمیت نباشد. اکنون مثال‌های دیگری از جملات مستقل از PA موجودند که این نقص را ندارند. این مثال‌ها عمدتاً به وسیلهٔ روش ابداعی دو منطق‌دان نامی، یعنی پریس[۴] و هرینگتون[۵]، به‌دست آمده‌اند و بیشتر خواص ترکیبیاتی اعداد (برای مثال شکلهایی از قضیهٔ رمزی) هستند. مراجع [K2] و [PH] در این زمینه خواندنی هستند. در هر حال باید متذکر شد که روش اخیر به اثبات استقلال جملاتی از نوع $\Pi_۲$ از PA می‌انجامد، در حالی‌که $\mathrm{Con(PA)}$ فرمولی $\Pi_۱$ است (برای تعریف $\Pi_۲$ و $\Pi_۱$، فصل ۵ را ببینید). یعنی قضیه‌های گدل استقلال جملاتی با پیچیدگی کمتر را نشان می‌دهند و این یک مزیت است.

---

[۴] Paris
[۵] Harington

۴. چند خاصیت مدلهای نااستاندهٔ PA

در این فصل پاره‌ای از خواص اساسی مدلهای نااستاندهٔ PA را ذکر می‌کنیم. مرجع اصلی، [K2] است. در همین‌جا متذکر می‌شوم که اطلاعات ما در مورد این مدل‌ها چندان زیاد نیست، یا بهتر است بگویم، نمی‌تواند باشد. دلیل این امر، قضیهٔ تننباوم[٦] است. بنابراین قضیه، مدل‌های نااستاندهٔ PA، بازگشتی نیستند. این به‌زبان غیر فنی یعنی اینکه توصیف صریح یا الگوریتمیک از عملهای $+$ و $\cdot$ در آنها نمی‌توان ارائه کرد. اگر M یک مدل نااستاندهٔ PA باشد، آن‌گاه M، $\mathbb{N}$ را به‌عنوان یک پارهٔ آغازی در بر دارد. در واقع اگر M شمارا باشد، از نظر ترتیب دارای شکل زیر خواهد بود:

$$\overbrace{\xrightarrow{\mathbb{N}}}^{\text{یک نسخه از } \mathbb{N}} \quad \overbrace{(\cdots \xleftrightarrow{\mathbb{Z}} \cdots \xleftrightarrow{\mathbb{Z}} \cdots \xleftrightarrow{\mathbb{Z}} \cdots)}^{\mathbb{Q} \text{ نسخه از } \mathbb{Z}}$$

دلیل این امر این است که، اگر $t \in M$ یک عنصر نااستانده (بی‌نهایت بزرگ) باشد، آنگاه عناصر

$$\ldots, t-۲, t-۱, t, t+۱, t+۲, \ldots$$

تشکیل یک $\mathbb{Z}$—زنجیر خواهند داد. اثبات اینکه این مجموعه از $\mathbb{Z}$—زنجیرها از نظر ترتیب با $\mathbb{Q}$ یکریخت است، متکی بر قضیهٔ سادهٔ Overspill است. بنابراین قضیه، در یک مدل نااستاندهٔ PA، هیچ برش سره‌ای تعریف پذیر نیست. اگر $M \models \mathrm{PA}$، $I \subsetneqq M$، I یک برش (سره) M است هرگاه I از پائین و همچنین تحت عمل تالی گرفتن، بسته باشد. اگر $a, b \in M$ نمایندهٔ دو $\mathbb{Z}$—زنجیر متفاوت در M باشند و $M \models a < b$، آنگاه $M \models \exists x(a+n < x \wedge x+n < b)$، به ازای هر عدد طبیعی n. پس بنابر قضیهٔ Overspill، عنصر نااستانده‌ای از M چون c موجود است که $M \models \exists x(a+c < x \ \wedge \ x+c < b)$. فرض کنید $d \in M$ چنان باشد که $M \models \ a+c < d \ \wedge \ d+c < b$، در اینصورت $\mathbb{Z}$—زنجیر مشخص شده توسط d بین $\mathbb{Z}$ — زنجیرهای مشخص شده توسط a و b قرار می‌گیرد. با کامل کردن جزئیات می‌توان دید که با یک مدل از نظریهٔ ترتیب‌های خطی چگال بدون

[٦] Tennenbaum

نقطهٔ ابتدایی و انتهایی (DLO) مواجه هستیم. دانسته است که هر مدل شمارای DLO با $(\mathbb{Q},<)$ یکریخت است.

اگر M مدلی ناشمارا از PA باشد، با تعویض $\mathbb{Q}$ با یک مدل مناسب DLO، تصویر مشابهی از ترتیب آن بدست می آید.

اینکه به‌ازای چه مدلهای $(A,<) \models \mathrm{DLO}$، جائیکه A ناشمارا است، مدلی از PA از این ترتیب وجود دارد، سؤالی باز می‌باشد. در مورد $(\mathbb{R},<)$، می‌دانیم که مدلی از PA از این ترتیب موجود نیست. برای دیدن مروری بر نتایج موجود و همچنین سؤالات باز در این زمینه [BK] را ببینید.

همانطور که قبلاً گفته شد، معرفی یک مدل نااستاندهٔ PA از طریق توصیف صریح عملهای آن ممکن نیست. در عین حال، اگر مدل نااستانده‌ای چون $M \models \mathrm{PA}$ داده شده باشد، می‌توان وجود توسیع‌های مناسب متفاوتی از M به مدلهای نااستاندهٔ دیگر PA را نشان داد.

در این‌جا چند تعریف مرتبط را متذکر می‌شوم:

فرض کنید $M, M' \models \mathrm{PA}$ (مدل‌ها و مجموعه‌های زمینهٔ آن‌ها را با نمادی مشابه نشان می‌دهیم.) M یک زیر مدل M' است، هرگاه $M \subseteq M'$ ، $0_M = 0_{M'}$، $1_M = 1_{M'}$ و همچنین M تحت $+_{M'}$ و $\cdot_{M'}$ بسته بوده و $<_M$، تحدید $<_{M'}$ به M باشد. معمولاً، نماد $M \subseteq M'$، برای نشان دادن این‌که M زیر مدل M' است به کار می‌رود. M یک زیر مدل مقدماتی M' است، هرگاه $M \subseteq M'$ و به ازای هر فرمول $\varphi(x_0, \ldots, x_n)$، و $a_0, \ldots, a_n \in M$، $M \models \varphi(a_0, \ldots, a_n)$ اگر و تنها اگر $M' \models \varphi(a_0, \ldots, a_n)$. این مفهوم با نماد $M \preccurlyeq M'$ نشان داده می‌شود.

M' یک توسیع هم پایان از M است، $M \subseteq_{cf} M'$، هرگاه

$$\forall a \in M' \; \exists b \in M (M' \models b \geqslant a)$$

M' یک توسیع انتهایی از M است، $M \subseteq_e M'$، هرگاه

$$\forall a \in M \; \forall b \in M' (M' \models b < a \Longrightarrow b \in M)$$

(در این حالت M را یک پارهٔ آغازی M' گویند.)

به ازای هر مدل نااستاندهٔ $M \models \mathrm{PA}$، مدل‌های $M', M'' \models \mathrm{PA}$ موجودند که $M \precneqq_{cf} M'$ و $M \precneqq_e M''$. به عبارت دیگر، توسیع‌های سرهٔ مقدماتی هم پایان و انتهایی از M (به مدل‌های دیگر PA) موجودند. در واقع می‌توان ثابت کرد که هر توسیع هم پایان از یک مدل PA به یک مدل PA، مقدماتی است. قضیهٔ جالب دیگر در این زمینه، قضیهٔ فریدمن است. بنابر این قضیه اگر $M \models \mathrm{PA}$ نااستانده و شمارا باشد و $a \in M$، آن‌گاه پارهٔ آغازی $I \subsetneqq_e M$ موجود است که $a \in I$ و I با M یکریخت است ($I \cong M$). در این حالت روشن است که $I \models \mathrm{PA}$. این قضیه وجود پاره‌های آغازی به اندازهٔ دلخواه بزرگ در یک مدل نااستاندهٔ PA را نشان می‌دهد که خود مدل PA هستند. از طرف دیگر، ثابت شده است که می‌توان پاره‌های آغازی به‌دلخواه کوچکی که PA را ارضاء کنند نیز یافت. در حالت فوق $I' \subseteq_e M$ موجود است که $a \notin I'$ و $I' \models \mathrm{PA}$.

در همین‌جا بحث کوتاه خود در مورد حوزهٔ وسیع مدل‌های نااستاندهٔ PA را به پایان می‌بریم. تنها متذکر می‌شویم که می‌توان PA را به کمک خواص نظریهٔ مدلی‌اش به طور منحصر به فرد مشخص کرد؛ برای دیدن این مطلب [K1] را ببینید. به نظر می‌رسد که مطالعهٔ زیر نظریه‌های PA، به خصوص زیر نظریه‌های ضعیف PA، امروزه از اهمیت بیشتری برخوردار است و توجه افراد بیشتری را به خود مشغول داشته است.

۵. زیر نظریه‌های PA

در این فصل به معرفی مختصر برخی نظریه‌های مهم PA می‌پردازیم. این زیر نظریه‌ها معمولاً با تحدید ردهٔ فرمول‌هایی که استقراء روی آن‌ها مجاز است و یا، تغییر شکل اصل استقراء به دست می‌آیند.

یک دلیل اساسی برای مطالعهٔ زیر نظریه‌های PA، تحقیق در مورد سؤالاتی به‌شکل زیر است:

" برای اثبات حکم حسابی φ، اثبات پذیر در PA، استفاده از چه مقدار قدرت PA ضروری است؟ "

دلیل مهم دیگر، ارتباطی است که رده‌هایی از این زیر نظریه‌ها با نظریهٔ پیچیدگی

محاسبه دارند. در ابتدا، به معرفی رده‌های مختلف فرمول‌های حسابی می‌پردازیم.

بنابر قضیهٔ شکل نرمال پیشوندی در منطق، هر فرمول حسابی با فرمولی به فرم

$$Q_1 x_1\, Q_2 x_2 \dots Q_n x_n \quad (\text{فرمولی بدون سور})$$

معادل است، جایی‌که Q_i، به ازای $1 \le i \le n$، نمایشگر سور $\exists$ یا $\forall$ می‌باشد. ردهٔ فرمول‌های بدون سور (باز) با Open نشان داده می‌شود. سورهای به شکل $\forall x < t$ یا $\exists x < t$، جایی‌که t یک ترم فاقد متغیر آزاد x است، سورهای محدود نامیده می‌شوند.

Δ_0 ردهٔ همهٔ فرمول‌های حسابی است که سورهای موجود در آن‌ها، همگی محدود هستند. فرض کنید $\varphi \in \Delta_0$. فرمول $\forall x_1 \dots \forall x_n\ \varphi$ یک فرمول Π_1 و فرمول $\exists x_1 \dots \exists x_n\ \varphi$ یک فرمول Σ_1 نامیده می‌شود. به‌همین ترتیب، اگر $\psi \in \Sigma_i$ آن‌گاه $\forall x_1 \dots \forall x_n\ \psi$ یک فرمول Π_{i+1} است و اگر $\theta \in \Pi_i$ آن‌گاه $\exists x_1 \dots \exists x_n\ \theta$ یک فرمول Σ_{i+1} است.

توجه کنید که در تعریف‌های فوق، n می‌تواند ۰ نیز باشد، پس به‌ازای هر n، $\Pi_n \subseteq \Sigma_{n+1}$ و $\Sigma_n \subseteq \Pi_{n+1}$ ضمناً $\Delta_0 = \Sigma_0 = \Pi_0$.

تعریف می شود:

$$I\mathrm{open} = \mathrm{PA}^- + \{I_x\varphi \mid \varphi\ \text{باز}\}, \quad I\Sigma_n = \mathrm{PA}^- + \{I_x\varphi \mid \varphi \in \Sigma_n\},$$
$$I\Pi_n = \mathrm{PA}^- + \{I_x\varphi \mid \varphi \in \Pi_n\}$$

برای سهولت در معرفی، تقسیم زیر نظریه‌های PA به زیر نظریه‌های بسیار ضعیف، ضعیف و قوی مناسب است. مراجع اصلی [Bus3]، [HP] و [K2] می‌باشند.

۱.۵. زیر نظریه‌های بسیار ضعیف PA

زیر نظریه‌هایی از PA که با حذف کامل اصل استقراء به‌دست می‌آیند، عمدتاً زیر نظریه‌های بسیار ضعیف PA را تشکیل می‌دهند.

برای مثال، می‌توان از PA^- یاد کرد. همان‌طور که قبلاً گفته شد، PA^- مجموعهٔ اصول موضوعهٔ قسمت‌های نامنفی حلقه‌های جابجایی و یک‌دار و به‌طور گسسته مرتب است

(گسسته مرتب یعنی آن‌که بین ۰ و ۱، و به‌طور معادل هر عدد و تالی آن، عددی وجود ندارد).

فرض کنید $\Sigma_1 - \mathrm{Th}(\mathbb{N}) = \{\sigma \mid \sigma \in \Sigma_1, \mathbb{N} \models \sigma\}$. در این‌صورت

$$\mathrm{PA}^- \vdash \Sigma_1 - \mathrm{Th}(\mathbb{N})$$

دلیل این امر آن است که هر مدل از PA^-، $\mathbb{N}$ را به‌عنوان یک پارهٔ آغازی دربردارد. به‌علاوه، می‌توان ثابت کرد که اگر $M \subseteq_e M'$، آن‌گاه به ازای هر $\sigma \in \Sigma_1$، $M \models \sigma \iff M' \models \sigma$. از طرف دیگر روشن است که این مطلب در مورد جملات Π_1 درست نیست، زیرا $\mathrm{Con(PA)}$ فرمولی Π_1 است. مثالی ساده که ضعف PA^- را نشان می‌دهد آن‌است که PA^- نمی‌تواند ثابت کند که هر عددی زوج یا فرد است:

$$\mathrm{PA}^- \not\vdash \forall x\, \exists y\, (x = 2y \vee x = 2y + 1)$$

برای دیدن این‌که چرا مطلب فوق درست است، توجه کنید که $\mathbb{Z}[t]^+ \models \mathrm{PA}^-$. $\mathbb{Z}[t]$ حلقه‌ای است که از افزودن عنصر جدید (بی‌نهایت بزرگ) t به $\mathbb{Z}$ پدید می‌آید. جمع و ضرب و ترتیب روی $\mathbb{Z}[t]$ همان‌گونه که در جبر تعریف می‌شوند، در نظر گرفته می‌شوند. ضمناً، $\mathbb{Z}[t]^+ = \{a \mid a \in \mathbb{Z}[t], a \geq 0\}$. در این مدل، عنصر t نه زوج است و نه فرد. توجه کنید که $\mathbb{Z}[t]^+$ به‌وضوح یک مدل بازگشتی است، دستورالعمل‌های مشخصی در مورد انجام اعمال + و . و هم‌چنین تشخیص ترتیب، وجود دارند. این، تفاوت عظیم PA^- و PA (که فاقد مدل نااستانداٰ بازگشتی است) را نشان می‌دهد.

زیر نظریهٔ بسیار ضعیف معروف دیگر، نظریهٔ Q است. این نظریه در زبان $\{0, s, +, \cdot\}$ ارائه می‌شود. s نشان‌گر تابع تالی است. نماد $\leq$ در زبان نیامده ولی می‌توان آن‌را به‌صورت $x \leq y \longleftrightarrow \exists z(x + z = y)$ تعریف کرد. نظریهٔ Q چیزی نیست جز همان خواص ابتدایی نمادهای موجود در زبانش. می‌توان نشان داد که $\mathrm{Iopen} \vdash Q$. از ذکر جزئیات در مورد این نظریه صرف نظر می‌کنیم.

خود نظریهٔ Iopen، هرچند که از استقراء بی‌بهره نیست، اما درعین حال مناسب‌تر است که جزو نظریه‌های بسیار ضعیف محسوب شود. یک دلیل این امر، وجود مدل‌های نااستانداٰ بازگشتی برای آن‌است. در واقع روش‌هایی که برای مطالعهٔ Iopen به‌کار رفته‌اند

به‌کلی با روش‌های بررسی زیرنظریه‌های ضعیف PA که بعداً مورد اشاره قرار می‌گیرند، متفاوت هستند. با این روش‌ها که عمدتاً جبری هستند، می‌توان تحلیل بسیار زیبایی از Iopen ارائه کرد.

۱.۱.۵ نظریهٔ استقرای باز (Iopen)

یادآوری می‌کنیم که Iopen زیرنظریه‌ای از PA است که از افزودن همهٔ موارد استقراء روی فرمول‌های باز (یعنی بدون سور) به PA^-، حاصل می‌شود. مطالعهٔ این نظریه در دههٔ ۱۹۶۰ میلادی توسط شفردسون آغاز شد. او محکی کاملاً جبری برای ساخت‌هایی که مدل Iopen هستند ارائه کرد و به‌کمک آن مدل بازگشتی معروف خود از این نظریه، یعنی $S_t(\mathbb{N})$، را ساخت.

قضیه ۱ (شفردسون) فرض کنید M حلقه‌ای جابجایی، یک‌دار و به‌طور گسسته مرتب باشد (به‌طور خلاصه $M \models \mathrm{DOR}$) و F میدان مرتب کسرهای M باشد. در این‌صورت دو شرط زیر معادل هستند:

i) $M^+ \models \mathrm{Iopen}$

ii) به‌ازای هر $r > ۰$ متعلق به $\mathrm{RC}(F)^+$ (عناصر مثبت متعلق به بستار حقیقی F)، وجود دارد $a \in M^+$، به‌طوری که $a \leq r < a + ۱$.

به‌عبارت دیگر، مدل‌های Iopen دقیقاً قسمت‌های مثبت مدل‌هایی از DOR هستند که هر عنصر مثبت متعلق به بستار حقیقی میدان کسرهای خود را با تقریب کم‌تر از یک تخمین می‌زنند. مدل شفردسون از Iopen شامل همهٔ عناصر به‌فرم

$$a_n t^{n/q} + a_{n-۱} t^{n-۱/q} + \ldots + a_۱ t^{۱/q} + a_۰$$

است، جایی‌که q عددی صحیح و مثبت، n عددی طبیعی (احتمالاً ۰) و $a_۰$ عددی صحیح است. ضمناً به‌ازای $i > ۰$، a_i متعلق به میدان اعداد جبری حقیقی ($\tilde{\mathbb{Q}}$) است. هم‌چنین فرض می‌شود که $a_n > ۰$، اگر $n > ۰$ و $a_۰ \geq ۰$، اگر $n = ۰$.

با قرار دادن $t > n$، به‌ازای هر عدد طبیعی n، ترتیب به‌طور طبیعی روی $S_t(\mathbb{N})$ القاء می‌شود. به‌سادگی می‌توان نشان داد که $S_t(\mathbb{N})$ هر عنصر متعلق به میدان سری‌های پوئیزو[۷] روی میدان اعداد جبری حقیقی، یعنی

$$(\tilde{\mathbb{Q}})\left((t^{\frac{1}{\infty}})\right) = \{a_n t^{n/q} + a_{n-۱} t^{n-۱/q} + \ldots + a_۰ + a_{-۱} t^{-۱/q} + \ldots \mid ۰ < q \in \mathbb{N}, n \in \mathbb{Z}, a_i \in (\tilde{\mathbb{Q}})\}$$

را با تقریب کم‌تر از یک تخمین می زند. می‌توان ثابت کرد که $\tilde{\mathbb{Q}}\left((t^{\frac{1}{\infty}})\right)$ یک میدان بستهٔ حقیقی است (قضیهٔ پوئیزو).

مدل شفردسون، برای مثال، نشان می‌دهد که $\mathrm{Iopen} \nvdash \mathrm{Irrational}(\sqrt{۲})$، یعنی

$$\mathrm{Iopen} \nvdash \forall x, y(x^۲ = ۲y^۲ \longrightarrow x = ۰)$$

دلیل این امر این است که، در این مدل، $(\sqrt{۲}t)^۲ = ۲(t^۲)$.

افراد دیگری چون ویلکی[۸]، مکینتایر[۹] ومارکر[۱۰] مطالعهٔ Iopen را ادامه دادند و مدل‌های مختلفی از Iopen با خواص مشخص ساختند، برای مثال [MM] و [Wilk] را ببینید. مجتبی منیری [M]، با تعمیم روش شفردسون، مدلی بازگشتی از Iopen ساخته است که شامل زیرمجموعه‌ای هم‌پایان از عناصر اول دوقلو است. بوگاتا[۱۱]، در سال ۱۹۹۱، ثابت کرد که Iopen متناهیاً اصل پذیر نیست (این خاصیتی است که PA هم دارا است، اما در مورد زیر نظریه های ضعیف، این سؤالی باز و اساسی است).

۲.۵. زیر نظریه‌های قوی PA

به‌ازای هر فرمول حسابی $\varphi(x)$، اصول استقراء، استقرای ترامتناهی، قانون کوچک‌ترین عدد و جایگزینی، به‌ترتیب به‌صورت زیر تعریف می‌شوند:

$$I\varphi:\ (\varphi(۰) \wedge (\forall x)(\varphi(x) \longrightarrow \varphi(x+۱))) \longrightarrow \forall x\, \varphi(x)$$

$$I^t\varphi:\ [\forall x\ ((\forall y < x)\, \varphi(y) \longrightarrow \varphi(x))] \longrightarrow \forall x\, \varphi(x)$$

[۷] Parson
[۸] Wilkie
[۹] Macintyre
[۱۰] Marker
[۱۱] Boughattas

$$L\varphi:\ (\exists x)\,\varphi(x)\ \longrightarrow\ \exists x\ (\varphi(x)\wedge\ (\forall y<x)\,\neg\,\varphi(y))$$

$$B\varphi:\ (\forall v)\ [(\forall x\leq v)\,\exists y\,\varphi(x,y)\ \longrightarrow\ (\exists v)(\forall x\leq v)\,(\exists y\leq v)\varphi(x,y)]$$

زیر نظریه‌های زیر از PA به کمک اصول فوق تعریف می‌شوند:

فرض کنید $n\geq ۰$.

$$\begin{aligned} I\Sigma_n &= \mathrm{PA}^-\cup\{I\varphi\,|\,\varphi\in\Sigma_n\}\\ I^t\Sigma_n &= \mathrm{PA}^-\cup\{I^t\varphi\,|\,\varphi\in\Sigma_n\}\\ L\Sigma_n &= \mathrm{PA}^-\cup\{L\varphi\,|\,\varphi\in\Sigma_n\}\\ B\Sigma_n &= \mathrm{PA}^-\cup\{B\varphi\,|\,\varphi\in\Sigma_n\} \end{aligned}$$

نظریه‌های $I\Pi_n$، $I^t\Pi_n$، $L\Pi_n$ و $B\Pi_n$، به‌طریق مشابه و با جایگزینی Π_n به‌جای Σ_n، حاصل می‌شوند. شکل زیر، وضعیت نظریه‌های فوق از نظر قدرت اثباتی را نشان می‌دهد. در مورد $B\Sigma_{n+۱}\Longrightarrow I\Sigma_{n+۱}$ و $I\Sigma_n\Longrightarrow B\Sigma_{n+۱}$ پیکان‌ها واقعاً یکطرفه هستند، یعنی $B\Sigma_{n+۱}\not\vdash I\Sigma_n$ و $I\Sigma_{n+۱}\not\vdash B\Sigma_{n+۱}$.

$$\begin{array}{lllllllllll} I\Sigma_{n+۱} \\ \Downarrow \\ B\Sigma_{n+۱} & \Longleftrightarrow B\Pi_n \\ \Downarrow \\ I\Sigma_n & \Longleftrightarrow I\Pi_n \Longleftrightarrow L\Sigma_n \Longleftrightarrow L\Pi_n \Longleftrightarrow I^t\Sigma_n \Longleftrightarrow I^t\Pi_n \end{array}$$

به‌ازای $n\geq ۱$، نظریه‌های فوق، زیر نظریه‌های قوی PA محسوب می‌شوند. ضعیف‌ترین آن‌ها، $I\Sigma_۱$ است ولی این نظریه آن‌قدر قدرت دارد که حسابی‌سازی نحو و ساخت فرمول $\mathrm{prov}(x,y)$، آن‌گونه که در قضایای گدل مورد نیاز است، را انجام دهد. نکتهٔ اساسی در این مورد آن است که تابع نمایی، یعنی $f(x,y)=x^y$، در $I\Sigma_۱$ تعریف پذیر است و به‌علاوه $I\Sigma_۱$ می‌تواند تام بودن این تابع را ثابت کند. به‌عبارت دیگر فرمول $\exp(z,x,y)$ متعلق به

Δ_0 وجود دارد که روی مجموعهٔ اعداد طبیعی، شبیه تابع نمایی $z = x^y$ رفتار می‌کند و ضمناً $I\Sigma_1$ توانایی اثبات خواص زیر برای آن را دارد:

$$(\exp(x,y,z_1) \wedge \exp(x,y,z_2)\ \longrightarrow\ z_1 = z_2,$$

$$\exp(x,0,1),$$

$$\exp(x,y,z)\ \longrightarrow\ \exp(x,y+1,xz)$$

$$(\exp(x,y,z) \wedge y' < y)\ \longrightarrow\ \exists z'\ \exp(x,y',z'),$$

$$\exp(x,y,z) \longrightarrow z \neq 0,$$

و سرانجام فرمولی که تام بودن تابع نمایی را بیان می‌کند، یعنی Exp:

$$\forall x, y\, \exists ! z\ \exp(x,y,z)$$

برای روشن شدن اهمیت تابع نمایی در قضایای گدل، توجه کنید که اگر فرمول $A(x)$ دارای m نماد و ترم t دارای n نماد باشد، آن‌گاه فرمول $A(t)$، که از جایگزینی یکنواخت t به‌جای موارد آزاد x در $A(x)$ به‌دست می‌آید، ممکن است دارای تعداد نمادهایی درحد mn باشد. در این‌صورت اگر یک کدگذاری گدلی مؤثر به‌کار رود، A دارای عدد گدل $g(A) \approx 2^{O(m)}$ و t دارای عدد گدل $g(t) \approx 2^{O(n)}$ و بنابراین، $A(t)$ دارای عدد گدل

$$g\left(A(t)\right)\ \approx 2^{O(n.m)}\ \approx \left(g(A)\right)^{O(n)}\ \approx \left(g(A)\right)^{O(\log_2(g(t)))}$$

خواهد بود. توجه کنید که مقدار $g\left(A(t)\right)$ توسط یک چندجمله‌ای برحسب $g(A)$ و $g(t)$ محدود نمی‌شود. بنابراین برای اثبات خواص کدگذاری گدلی به‌صورت صوری، استفاده از تابع نمایی (یا حداقل تابع $f(x,y) = x^{\log_2 y}$ که سرعت رشدی کم‌تر از تابع نمایی دارد، ولی همچنان توسط هیچ چند جمله‌ای برحسب y, x مهار نمی‌شود) ضروری است. مقالهٔ توصیفی [Bus 4] در این مورد خواندنی است. در بخش بعد خواهیم دید که برای مثال، $I\Delta_0$ توانایی اثبات Exp را ندارد، هرچند که مابقی خواص exp در $I\Delta_0$ بیان پذیر و قابل اثبات است. بنابراین صوری‌سازی نحو در $I\Delta_0$ با مشکلی اساسی مواجه است.

قضیه زیر نشان می دهد که سلسله مراتب زیر نظریه های قوی حساب سره است.

قضیه ۲ فرض کنید $n \geq 1$.

۱) $I\Sigma_{n+1} \vdash \mathrm{Con}(I\Sigma_n)$

۲) $I\Sigma_n \nvdash \mathrm{Con}(I\Sigma_n)$

برای دیدن خواص مدل‌های نااستانده‌ٔ این نظریه‌ها، [HP] و [D] را ببینید. برای مثال قضیهٔ زیر را داریم:

قضیه ۳ به‌ازای هر $n \geq 2$، اگر $M \models I\Sigma_n$ آن‌گاه توسیعی سره، Σ_n—مقدماتی و انتهایی از M موجود است.

M' توسیعی Σ_n—مقدماتی از M است هرگاه شرط مذکور برای مقدماتی بودن توسیعها، برای فرمولهای عضو Σ_n (نه لزوماً برای همهٔ فرمولها) برقرار باشد.
قبل از اتمام این بخش، قضیهٔ مشهور موجود درمورد مشخص سازی توابع اثبات پذیرتام در $I\Sigma_1$ را ذکر می‌کنیم. این قضیه اول بار توسط پارسونز[۱۲] در ۱۹۷۰ ثابت شده و بعداً اثبات‌های متفاوتی برای آن ارائه شده است.

تعریف ۴ فرض کنید T یک نظریهٔ حسابی باشد. گوییم تابع $f : \mathbb{N}^k \longrightarrow \mathbb{N}$ در T، Σ_1—تعریف‌پذیر است هرگاه فرمول $\Phi(\vec{x}, y)$ موجود باشد، جایی‌که $\Phi \in \Sigma_1$ و Φ به‌جز $y, \vec{x}$ متغیر آزاد دیگری ندارد، به‌طوری‌که:

i) به‌ازای هر $\vec{n} \in \mathbb{N}^k$، $\Phi(\vec{n}, f(\vec{n}))$ (در مدل استانده) درست باشد.

ii) $T \vdash \forall \vec{x}\, \exists! y\, \Phi(\vec{x}, y)$

$\vec{x}$ نمایشگر دنباله‌ای متناهی از متغیرها است و $\exists! y$ به معنی "دقیقاً یک y وجود دارد" است. توابع Σ_1—تعریف‌پذیر یک نظریه، معمولاً توابع اثبات‌پذیر تام یا اثبات‌پذیر بازگشتی آن نظریه نیز نامیده می‌شوند.

---
[۱۲] Parson

قضیه ۵ توابع Σ_1–تعریف‌پذیر $I\Sigma_1$ دقیقاً توابع بازگشتی اولیه هستند.
یادآوری می‌کنم که توابع بازگشتی اولیه، توابعی از $\mathbb{N}^k$ به $\mathbb{N}$، $k \geq 1$، هستند که از تابع ثابت ۰ و تابع تالی، با استفاده از عمل‌های ترکیب، تصویر و هم‌چنین استفاده از تعاریف بازگشتی به‌دست می‌آیند.

این‌که توابع بازگشتی اولیه در $I\Sigma_1$، Σ_1 تعریف‌پذیر هستند، اساساً توسط گدل اثبات شده است. در مورد مشخص‌سازی توابع اثبات‌پذیر تام نظریه‌های $I\Sigma_n$ و PA، نتایج مختلفی در دست است که از ذکر آن‌ها صرف‌نظر می‌شود.

۳.۵. زیر نظریه‌های ضعیف PA (حساب‌های ضعیف) و نظریهٔ پیچیدگی

در این قسمت، به معرفی زیر نظریه‌های ضعیف PA می‌پردازیم. از آن‌جا که مطالعهٔ این نظریه‌ها، اساساً به‌خاطر ارتباط آن‌ها با نظریهٔ پیچیدگی محاسبه انجام شده، دانستن مقدمات این نظریه برای فهم نتایج موجود درمورد حساب‌های ضعیف، ضروری است.
$I\Delta_0$، یا حساب محدود، یکی از زیر نظریه‌های ضعیف PA است. مطالعهٔ این زیر نظریه توسط روهیت پریخ[۱۳] آغاز شد. قضیهٔ اساسی‌ای که پریخ درمورد $I\Delta_0$ ثابت کرد این است:

قضیه ٦ (پریخ،۱۹۷۱) فرض کنید $A(x,y) \in \Delta_0$ و $I\Delta_0 \vdash \forall x\, \exists y\, A(x,y)$. در این‌صورت اعداد طبیعی مثبت l و k موجودند که $I\Delta_0 \vdash \forall x\, \exists y\, (y < x^k + l \wedge A(x,y))$.
و به‌طور کلی‌تر، اگر $I\Delta_0 \vdash \forall \vec{x}\, \exists y\, B(\vec{x},y)$، جایی‌که $B(\vec{x},y) \in \Delta_0$، آن‌گاه ترم t موجود است که

$$I\Delta_0 \vdash \forall \vec{x}\, \exists y \leq t\ B(\vec{x},y)$$

نتیجه ۷ تابع $f(\vec{x}) : \mathbb{N}^k \longrightarrow \mathbb{N}$ در $I\Delta_0$، Σ_1– تعریف پذیر است اگر و تنها اگر فرمول محدود چون $\Phi(\vec{x},y)$ (بدون متغیر آزادی جز $\vec{x}$ و y) و ترم $t(\vec{x})$ موجود باشند به طوری که $\Phi(\vec{n}, f(\vec{n}))$، به‌ازای هر $\vec{n} \in \mathbb{N}^k$، درست باشد و $I\Delta_0 \vdash \forall \vec{x}\, \exists! y \leq t\, \Phi(\vec{x},y)$.

[۱۳] Parikh

برای دیدن یک اثبات سادهٔ نظریهٔ مدلی مبتنی بر قضیهٔ فشردگی از قضیهٔ پریخ، [Kr,Th.5.1.4] را ببینید. [Bus3,1.4.3] حاوی اثباتی نظریهٔ برهانی برای این قضیه است.

از قضیهٔ پریخ نتیجه می‌شود که تابع نمایی، $x^y = z$، در $I\Delta_0$، Σ_1–تعریف‌پذیر نیست. این محدودیتی اساسی برای صوری کردن بسیاری از ساختارها در $I\Delta_0$ پدید می آورد.[۱۴]

بعد از کارهای اولیهٔ پریخ، افراد سرشناس زیادی به کار درمورد حساب محدود و ارتباط آن با سایر شاخه‌ها پرداختند، از قبیل ویلکی، پریس و باس. برای مثال [WP] و [Bus1] را ببینید.

۱.۳.۵ چند کلمه درمورد نظریهٔ پیچیدگی

نظریهٔ پیچیدگی محاسبه به بررسی پیچیدگی مسائل از جهت فضا (حافظه) و یا زمان (تعداد مراحل) لازم برای حل آن‌ها به‌صورت الگوریتمی و به‌وسیلهٔ کامپیوتر، می‌پردازد. در این‌جا ما تنها به پیچیدگی زمانی می‌پردازیم.

یک ماشینی تورینگ[۱۵]، نوع خاصی از یک کامپیوتر ایده‌آل، با حافظه‌ای بالقوه نامتناهی است. می‌توان توصیفی صریح و دقیق از ماشین‌های تورینگ ارائه کرد. معمولاً هنگامی که صحبت از پیچیدگی یک مسئله می‌شود، منظور، پیچیدگی حل آن به‌وسیلهٔ یک ماشین تورینگ است. در واقع ثابت شده است که هرچند این ماشین‌ها بسیار ساده هستند، اما از نظر مقاصد مربوط به نظریهٔ پیچیدگی، ماشین‌های تورینگ به‌اندازهٔ دیگر کامپیوترها قوی هستند.

یک ماشین تورینگ با یک ورودی خاص، بعد از تعدادی مرحلهٔ عملیات، در وضعیت accept یا reject متوقف می‌شود؛ و یا این‌که بی‌وقفه به‌کار ادامه خواهد داد. با استفاده از یک کدگذاری مؤثر، می‌توان تنها مسائلی به‌شکل $x \overset{?}{\in} A$، جایی‌که $A \subseteq \mathbb{N}$ ، را درنظر گرفت. فرض می‌شود که x به‌صورت دودویی به ماشین وارد می‌شود. $|x|$ نشان‌گر طول x، یعنی تعداد ارقام x در شکل دودویی آن است. داریم $|x| = \lceil \log_2(x+1) \rceil$ اگر $x > 0$، و

[۱۴] البته پریخ این ضعف را امتیازی برای نظریهٔ $I\Delta_0$ می‌داند و دلیلی برای نزدیک‌تر بودن آن به یک نظریهٔ ایده‌آل از نظر محاسبه‌پذیری (feasiblity)، نسبت به نظریه‌هایی که تام بودن تابع نمایی را ثابت می‌کنند.

[۱۵] Turing

$0 = |0|$. توجه کنید که $\lceil \log_2 x \rceil = y \iff 2^{y-1} < x \leq 2^y$.
ردهٔ پیچیدگی P، مجموعهٔ همهٔ زیرمجموعه‌هایی از $\mathbb{N}$ است که به‌صورت چندجمله‌ای تصمیم‌پذیر هستند. به‌عبارت دیگر، زیر مجموعهٔ A از $\mathbb{N}$ به P تعلق دارد، هرگاه ماشین تورینگ M_A و تابع چندجمله‌ای f موجود باشند به‌طوری‌که به‌ازای هر ورودی $n \in \mathbb{N}$، M_A در حداکثر $f(|n|)$ مرحله متوقف شود، و ضمناً:

$$n \in A \iff \text{با ورودی } n \text{ در وضعیت accept متوقف می‌شود } M_A$$

مسائل از نوع P، یعنی مسائلی که در زمان چند جمله‌ای قابل حل هستند، از اهمیت زیادی برخوردارند، زیرا تنها مسائلی هستند که "به‌طور عملی" توسط کامپیوترها قابل حل‌اند. حتی این‌گونه مسائل هنگامی‌که درجهٔ چندجمله‌ای تعیین کننده‌ی پیچیدگی آن‌ها بالا باشد، به‌طور مؤثر قابل حل نیستند، زیرا زمان لازم برای این کار ممکن است نجومی باشد. اما در این زمینه فرضیه‌ای وجود دارد که بیان می‌کند:

فرضیهٔ محاسبه پذیری عملی (feasibility): یک مسئله دارای حل مؤثر و عملی است اگر و تنها اگر به‌صورت چندجمله‌ای قابل حل باشد.

برای توضیح بیشتر در این زمینه به مقالهٔ توصیفی [C] از کوک[۱۶]، یکی از بنیان‌گزاران نظریهٔ پیچیدگی، مراجعه کنید. یک ماشین تورینگ نامعین، عبارت است از یک ماشین تورینگ که مراحل کار آن به‌طور معین در نظر گرفته نشده است. به‌عبارت دیگر، یک چنین ماشینی با یک ورودی خاص در هر مرحله از کار، امکان ادامهٔ کار به طرق مختلفی را (به‌طور هم‌زمان) دارد.

یک ماشین تورینگ نامعین چندجمله‌ای، ماشین تورینگ نامعینی است که برای آن تابع چندجمله‌ای g موجود باشد به‌طوری‌که، به ازای هر ورودی m، همهٔ شاخه‌های کار آن، در زمان حداکثر $g(|m|)$ (در وضعیت accept یا reject) متوقف شوند.

NP ردهٔ همهٔ زیرمجموعه‌هایی از $\mathbb{N}$ چون A است به طوری که برای آن‌ها ماشین تورینگ نامعین چندجمله‌ای M_A موجود است به‌گونه‌ای که $m \in A$ اگر و تنها اگر حداقل یکی از شاخه‌های کاری M_A با ورودی m در وضعیت accept متوقف شود.

[۱۶] Cook

روشن است که $\mathrm{P} \subseteq \mathrm{NP}$. سؤال باز و بسیار مهم درمورد تساوی این دو است، آیا $\mathrm{P} = \mathrm{NP}$؟ اهمیت این سؤال در این است که درمورد تعداد بسیار زیادی از مسائل مهم که می‌دانیم در NP هستند، هنوز روشن نیست که آیا این مسائل در P نیز هستند یا نه؟ یعنی، آیا به‌صورت مؤثر قابل حل هستند یا نه؟ برای مثال مسألهٔ تصمیم SAT، یعنی اینکه آیا فرمول گزاره‌ای دلخواه داده شده ای ارضاء پذیر است یا نه، به این رده از مسائل تعلق دارد.

قرار می‌دهیم $\Sigma_{\circ}^{p} = \mathrm{P}$ و $\sum_{i+1}^{p} = \mathrm{NP}(\sum_{i}^{p})$ به‌ازای $i \geq \circ$. $\mathrm{NP}(\sum_{i}^{p})$ مجموعهٔ همهٔ زیرمجموعه‌هایی از $\mathbb{N}$ است که به‌وسیلهٔ یک ماشین تورینگ نامعین چند جمله‌ای که به یکی از اعضای Σ_i^p به‌عنوان اراکل دسترسی دارد، مشخص می‌شوند. مجموعهٔ A یک اراکل برای یک ماشین تورینگ M است هرگاه، M در هر لحظه بتواند از اطلاعات مربوط به عضویت در A استفاده کند.

توجه کنید که $\Sigma_{1}^{p} = \mathrm{NP}$. مجموعهٔ همهٔ Σ_i^p ها، $i \geq \circ$، سلسله مراتب زمان چندجمله‌ای (Polynomial Time Hierachy یا به‌طور مختصر PH) را می‌سازند،

$$\mathrm{PH} = \bigcup_{i=\circ}^{\infty} \Sigma_i^p$$

سلسله مراتب زمان خطی (Linear Time Hierachy یا Lin H) به نحو مشابه تعریف می‌شود:

$$\text{Lin Time} = \Sigma_{\circ}^{l} \text{ و } \Sigma_{i+1}^{l} = \text{NLin Time}(\Sigma_i^l)\text{، } i \geq \circ\text{، و } \text{Lin H} = \bigcup_{i\geq \circ}^{\infty} \Sigma_i^l.$$

فرض کنید که $\Delta_{\circ}^{\mathbb{N}}$ مجموعهٔ همهٔ روابطی روی مجموعهٔ اعداد طبیعی باشد که به‌وسیلهٔ فرمول‌هایی کراندار (در زبان حساب) تعریف‌پذیر هستند. برای مثال، رابطهٔ $\mathrm{Prime}(x)$ (x یک عدد اول است) به $\Delta_{\circ}^{\mathbb{N}}$ تعلق دارد زیرا در $\mathbb{N}$ درست است که:

$$\mathrm{Prime}(x) \longleftrightarrow 1 < x \wedge \forall y \leqslant x \, \forall z \leqslant x \, (y.z = x \longrightarrow (y = 1 \vee z = 1))$$

حقیقت جالبی که در این مورد وجود دارد این است که $\Delta_{\circ}^{\mathbb{N}} = \text{Lin H}$ (توجه کنید که در این‌جا، یک رابطه روی $\mathbb{N}$، که در واقع زیرمجموعه‌ای از یک $\mathbb{N}^k$ است، با مجموعهٔ کدهای اعضایش یکی گرفته شده است. این کدگذاری به‌وسیلهٔ فرمول‌های محدود قابل بیان است و خواص آن، حتی در $I\Delta_{\circ}$، قابل اثبات‌اند).

گوییم PH فرو می‌ریزد هرگاه $i \geqslant 0$ موجود باشد به‌طوری که $\Sigma^p_j = \Sigma^p_i$ به‌ازای هر j به‌طوریکه $i \geqslant j$. این که آیا PH فرو می‌ریزد یا نه، خود سؤالی باز و اساسی در نظریهٔ پیچیدگی است. سؤالات مشابهی درمورد Lin H وجود دارد. به مورد PH در بخش بعدی می‌پردازیم، اما در مورد Lin H اشاره می‌کنم که سؤال منطقیِ نظیرِ مسئلهٔ فرو ریزش این سلسله، سؤال $E^{\mathbb{N}}_1 \stackrel{?}{=} \Delta^{\mathbb{N}}_0$ است. E_1 مجموعهٔ همهٔ فرمول‌های به شکل $\exists x_n < t_n \ldots \exists x_1 < t_1 \varphi$ است، جایی‌که φ فرمولی بدون سور و t_i ترمی فاقد x_i است.

مسئلهٔ مرتبط دیگر، سؤال $IE_1 \stackrel{?}{\vdash} I\Delta_0$ است. IE_1 اول بار توسط ویلمر[۱۷] مورد مطالعه قرار گرفت. ویلمر ثابت کرد که IE_1 فاقد مدل نااستاندهٔ بازگشتی است، [Wilm] را ببیند.

۲.۳.۵ حساب‌های ضعیف و پیچیدگی محاسباتی

ثابت شده است که تابع $|x|$ در $I\Delta_0$، Δ_0- تعریف‌پذیر است. هم‌چنین فرمول محدود $\phi(x, y, z)$ وجود دارد که $I\Delta_0$ همهٔ خواص معمول تابع نمایی $x^y = z$، به‌جز تام بودن، را برای آن اثبات می‌کند. از طرف دیگر، اگر $M \models I\Delta_0$ آن‌گاه مجموعهٔ کدهای اعضای M، لزوماً تحت ضرب بسته نیست. به‌عبارت دیگر، اگر بخواهیم طول یک عنصر $x \in M$ را به‌صورت چند جمله‌ای افزایش دهیم (آنچنان‌که در محاسبهٔ چند جمله‌ای با ماشین تورینگ مورد نیاز است) حاصل کار لزوماً کد عضوی از M نخواهد بود. بنابراین برای صوری کردن محاسبهٔ چند جمله‌ای، نیاز به نظریه‌ای قویتر از $I\Delta_0$ است. معلوم شده است که اصل

$$\Omega_1 : \forall x, y \, \exists z \;\; x^{|y|} = z$$

دقیقاً چیزی است که در این مورد باید به $I\Delta_0$ اضافه شود.

یک تحول مهم در زمینهٔ مطالعهٔ حساب‌های ضعیف و ارتباط آن‌ها با نظریهٔ پیچیدگی، با معرفی نظریه‌های جدیدی (که اساساً زیر نظریه‌های $I\Delta_0 + \Omega_1$ ولی در زبانی توسعه یافته هستند) توسط ساموئل باس در تز دکترایش (Princeton 1985) به‌وجود آمد. این تز بعداً به‌صورت [Bus1] چاپ شد. این نظریه‌ها در زبان جدید $\{0, s, +, ., \#, |x|, \lfloor \frac{1}{2}x \rfloor\}$

---

[۱۷] Wilmer

مطرح شده‌اند. $x\#y$ (x اسمش y) نمایانگر $۲^{|x||y|}$ است.

رده‌های Σ_i^b و Π_i^b از فرمول‌های محدود در این زبان به‌صورت زیر تعریف می‌شوند:

۱) $\Sigma_۰^b = \Pi_۰^b$ مجموعهٔ همهٔ فرمول‌هایی هستند که سورهای موجود در آن‌ها همگی اکید می‌باشند، یعنی به‌شکل $\forall x < |t|$ یا $\exists x < |t|$ هستند.

۲) $\Sigma_{i+۱}^b$ و $\Pi_{i+۱}^b$، کوچک‌ترین مجموعه‌هایی هستند که در شرایط زیر صدق می‌کنند:

a) $\Sigma_i^b, \Pi_i^b \subseteq \Sigma_{i+۱}^b$ و $\Sigma_i^b, \Pi_i^b \subseteq \Pi_{i+۱}^b$.

b) اگر $\varphi \in \Sigma_{i+۱}^b$، آن‌گاه $\exists x \leq t\varphi \in \Sigma_{i+۱}^b$ و $\forall x \leqslant |t|\varphi \in \Sigma_{i+۱}^b$.
اگر $\varphi \in \Pi_{i+۱}^b$، آن‌گاه $\forall x \leq t\varphi \in \Pi_{i+۱}^b$ و $\exists x \leq |t|\varphi \in \Pi_{i+۱}^b$.

c) اگر $\varphi, \psi \in \Sigma_{i+۱}^b$، آن‌گاه $(\varphi \wedge \psi) \in \Sigma_{i+۱}^b$ و $(\varphi \vee \psi) \in \Sigma_{i+۱}^b$.
اگر $\varphi, \psi \in \Pi_{i+۱}^b$، آن‌گاه $(\varphi \wedge \psi) \in \Pi_{i+۱}^b$ و $(\varphi \vee \psi) \in \Pi_{i+۱}^b$.

d) اگر $\varphi \in \Sigma_{i+۱}^b$ و $\psi \in \Pi_{i+۱}^b$، آن‌گاه $\neg\psi$ و $(\psi \longrightarrow \varphi)$ در $\Sigma_{i+۱}^b$ هستند.
اگر $\varphi \in \Pi_{i+۱}^b$ و $\psi \in \Sigma_{i+۱}^b$، آن‌گاه $\neg\psi$ و $(\psi \longrightarrow \varphi)$ در $\Pi_{i+۱}^b$ هستند.

رده‌های فوق به‌گونه‌ای تعریف شده‌اند که قضیهٔ زیر درمورد آن‌ها درست باشد:

قضیه ۸ فرض کنید $i \geq ۱$. زیرمجموعهٔ A از مجموعهٔ اعداد طبیعی به ردهٔ پیچیدگی Σ_i^p تعلق دارد اگر و تنها اگر، فرمولی در Σ_i^b موجود باشد که زیرمجموعه‌ای از $\mathbb{N}$ که به‌وسیلهٔ آن تعریف می‌شود، برابر با A باشد.

BASIC نظریه‌ای است شبیه Q، در زبان جدید، که خواص اولیهٔ نمادها را بیان می‌کند. برای مثال $|x\#y| = s(|x|.|y|)$ و $x \neq ۰ \longrightarrow |x| = s(|\lfloor \frac{۱}{۲}x \rfloor|)$، دو عضو BASIC هستند. استقرای چند جمله‌ای، PIND، به‌صورت زیر تعریف می‌شود:

$$\left[A(۰) \wedge \forall x \left(A(\lfloor \frac{۱}{۲}x \rfloor) \longrightarrow A(x)\right)\right] \longrightarrow \forall x A(x).$$

تعریف ۹ به‌ازای $i \geq ۰$، $S_۲^i$ نظریه‌ای است که دارای اصول موضوع BASIC همراه با PIND روی همهٔ فرمول‌های Σ_i^b است. هم‌چنین $S_۲ = \bigcup_i S_۲^i$.

هنوز معلوم نیست که آیا دنبالهٔ $S_2^1 \subseteq S_2^2 \subseteq \ldots$ اکید است یا نه؟ یعنی، آیا $S_2^i \neq S_2^{i+1}$ برای هر i؟

نظریه‌های دیگری نیز در این زمینه به‌وسیلهٔ باس و دیگران معرفی شده‌اند که از ذکر آن‌ها صرف‌نظر می‌شود.

قضیه ۱۰ S_2 توسیعی محافظه‌کارانه از $I\Delta_0 + \Omega_1$ است. به‌عبارت دیگر، اگر φ فرمولی متعلق به زبان معمولی حساب باشد، آنگاه $I\Delta_0 + \Omega_1 \vdash \varphi$ اگر و تنها اگر $S_2 \vdash \varphi$.

قضیه ۱۱ دنبالهٔ $S_2^1 \subseteq S_2^2 \subseteq \ldots$ از حساب‌های ضعیف را در نظر بگیرید. اگر PH فرو نریزد، آن‌گاه این دنباله اکید است، یعنی به‌ازای هر $i \geq 1$، $S_2^i \neq S_2^{i+1}$. هم‌چنین، اکید بودن دنبالهٔ فوق معادل با به‌طور متناهی اصل‌پذیر نبودن S_2 است، که خود معادل با به‌طور متناهی اصل‌پذیر نبودن $I\Delta_0$ است.

قضیه ۱۲ S_2 به‌طور متناهی اصل‌پذیر نیست اگر و تنها اگر مدلی چون $M \models S_2$ موجود باشد به‌طوری‌که به‌ازای هر i، زیرمجموعه‌های تعریف‌پذیر (با پارامتر) M به‌وسیلهٔ فرمول‌های Σ_{i+1}^b اکیداً بیشتر از زیرمجموعه‌های تعریف‌پذیر (با پارامتر) به‌وسیلهٔ فرمول‌های Σ_i^b باشند.

باس، هم‌چنین توصیف دقیقی از توابع اثبات‌پذیر تام نظریه‌های S_2^i ارائه نموده است. جالب‌ترین قسمت، مورد مشخص‌سازی توابع اثبات‌پذیر تام S_2^1 است (که در این حالت به‌صورت توابع Σ_1^b- تعریف‌پذیر S_2^1 تعریف می‌شوند.)

قضیه ۱۳ توابع Σ_1^b- تعریف‌پذیر S_2^1 دقیقاً توابع محاسبه‌پذیر در زمان چند جمله‌ای هستند. (توجه کنید که در این‌جا با نوع نسبتاً متفاوتی از ماشین‌های تورینگ مواجهیم.)

برای قضایای فوق می توانید به مراجع [HP] و [Kr] مراجعه کنید. هم‌چنین ارتباط‌های جالبی بین S_2^1 و نظریهٔ پیچیدگی اثبات‌ها در منطق گزاره‌ها وجود دارد، [Bus2] شامل

مروری بر نتایج در این زمینه است. توجه کنید که خود منطق گزاره‌ها از طریق قضیهٔ زیر (اثبات شده توسط کوک) در ارتباط مستقیم با سؤالات اساسی نظریهٔ پیچیدگی قرار می‌گیرد. قبلاً یادآوری می‌کنم که coNP نمایشگر مجموعهٔ همهٔ متمم‌های اعضای NP است. یک سؤال اساسی در نظریهٔ پیچیدگی، $\mathrm{NP} \stackrel{?}{=} \mathrm{coNP}$ است. به‌سادگی می‌توان دید که اگر $\mathrm{NP} \neq \mathrm{coNP}$ آن‌گاه $\mathrm{P} \neq \mathrm{NP}$. هم‌چنین متذکر می‌شوم که در نظریهٔ پیچیدگی اثبات، طول یک گزاره برابر با تعداد رخ‌داد نمادها (متغیرها، رابطه‌های منطقی و پرانتزها) در آن و طول یک دنباله از گزاره‌ها (مثلاً یک برهان)، برابر با مجموع طول گزاره‌های ظاهرشده در آن است.

قضیه ۱۴ $\mathrm{NP} = \mathrm{coNP}$ اگر و تنها اگر دستگاهی اثباتی برای منطق گزاره‌ها موجود باشد به‌طوری که در آن هر راستگو دارای اثباتی کوتاه باشد (یعنی چندجمله‌ای $p(x)$ وجود داشته باشد که هر راستگو τ دارای اثباتی با اندازهٔ کمتر از $p(|\tau|)$ در این دستگاه باشد).

٦. حساب شهودگرایی و زیرنظریه‌های آن

در این فصل انتهایی به معرفی مختصر حساب شهودگرایی و زیرنظریه‌های آن می‌پردازیم. مرجع اصلی درمورد این حساب و هم‌چنین منطق شهودگرایی، [TD] است.

منطق شهودگرایی با حذف اصل طرد شق ثالث، $A \vee \neg A$، از منطق کلاسیک به‌دست می‌آید. منطق شهودگرایی یکی از منطق‌های به‌اصطلاح ساختنی است و در واقع یکی از مهم‌ترین آن‌ها است.

برای توجیه نام ساختنی، شاید بیان دو خاصیت زیر از منطق شهودی کافی باشد:

(i) خاصیت فصلی (DP): اگر $\vdash_i A \vee B$، آن‌گاه $\vdash_i A$ یا $\vdash_i B$.

(ii) خاصیت وجودی (ED): اگر $\vdash_i \exists x A(x)$، آن‌گاه ترم بسته‌ای چون t در زبان موجود است که $\vdash_i A(t)$.

توجه کنید که $\vdash_i$، اثبات‌پذیری در منطق شهودگرایی مرتبهٔ اول (IQC) را بیان می‌کند. نظیر

شهودگرایی PA، حساب شهودگرایی یا حساب هیتینگ (HA) است که به وسیلهٔ هیتینگ[۱۸] در سال ۱۹۳۰ معرفی شد و مورد مطالعه قرار گرفت.

می‌توان ثابت کرد که HA نیز دو خاصیت DP و ED را دارا است. به‌علاوه می‌دانیم که به‌ازای هر فرمول $\varphi \in \Pi_2$، اگر $\mathrm{PA} \vdash \varphi$ آن‌گاه $\mathrm{HA} \vdash \varphi$. هم‌چنین، HA همهٔ نتایج PA را که به‌صورت فرمول‌هایی فاقد $\exists$ و $\vee$ باشند، ثابت می‌کند.

مطالعهٔ زیرنظریه‌های HA، به‌طور نظام‌مند، کاری نسبتاً جدید است. وهمایر[۱۹] دو نظریهٔ $i\Sigma_1$ و $i\Pi_1$ از HA را، که به‌ترتیب نظیر شهودگرایی $I\Sigma_1$ و $I\Pi_1$ می‌باشند مورد مطالعه قرار داد و برای مثال، ثابت کرد که $i\Sigma_1 \nvdash i\Pi_1$ و $i\Pi_1 \nvdash i\Sigma_1$، [We] را ببینید. برای نشان دادن آن‌که $i\Pi_1 \nvdash i\Sigma_1$؛ وهمایر ثابت کرد $i\Sigma_1 \vdash \forall x, y\, \exists z\, x^y = z$ ولی $i\Pi_1 \nvdash \forall x, y\, \exists z\, x^y = z$. در [M1] نشان داده شده است که $i\Pi_1 \nvdash \neg\neg\forall x, y\, \exists z\, x^y = z$. توجه کنید که درمورد نظریه‌های مبتنی بر منطق شهودگرایی، در حالت کلی، $\neg\neg A$ بسیار ضعیف‌تر از A است. نظریه‌های $i$open، $i\forall_1$ و $i\Pi_1$، هم‌چنین در [MOMO] مورد مطالعه قرار گرفته‌اند.

ثابت شده است که قضیهٔ شکل نرمال پیشوندی در منطق کلاسیک، در منطق شهودگرایی معتبر نیست. به‌عبارت دیگر، چنین نیست که هر فرمول دلخواه، در منطق شهودگرایی، معادل با فرمولی به‌شکل

$$(Q_n x_n) \ldots (Q_1 x_1) A$$

است، جایی‌که Q_i سور $\exists$ یا $\forall$، و A فرمولی فاقد سور است. این مطلب در حساب شهودگرایی نیز صحیح است. معلوم شده است که iPNF، یعنی HA با اصل استقراء تحدید شده به فرمول‌های پیشوندی، بسیار ضعیف‌تر از خود HA است. برای مثال، ویسر[۲۰] و وهمایر ثابت کرده‌اند که؛ iPNF توسیعی Π_2 ـ محافظه‌کارانه از $i\Pi_2$ است، [We] را ببینید.

و. بور [Bur] اخیراً زیرنظریه‌های جدیدی از HA (در زبان معمولی حساب) را معرفی و مورد مطالعه قرار داده است. بور پیچیدگی فرمول‌ها را نه برحسب سورها بلکه برحسب تعداد روابط $\longrightarrow$ موجود در آن‌ها درنظر گرفته است. خانوادهٔ $\{\phi_n \ :\ n \geq 0\}$ یکی از

---

[۱۸] Heyting
[۱۹] Wehmeier
[۲۰] Visser

خانوادهٔ فرمول‌هایی است که بور معرفی کرده است. او ثابت کرده که هر فرمول حسابی، در $i\Delta_0$ معادل با یک از این فرمول‌هاست. ضمناً $I\Sigma_n$ توسیعی Π_2 ـ محافظه‌کارانه از $i\phi_n$ است و هم‌چنین $I\Sigma_n \equiv_c I\phi_n$، به‌ازای $n \geq 0$. نظیر شهودگرایانهٔ نظریه‌های باس نیز مورد مطالعه قرار گرفته‌اند. برای مثال، کوک و ارکهارت[۲۱] [CU] ثابت کرده‌اند که اگر $IS_2^1 \vdash \forall \vec{x}\ \exists y\ \varphi(\vec{x}, y)$، جایی‌که IS_2^1 نظیر شهودگرایانهٔ S_2^1 است، آن‌گاه تابع محاسبه‌پذیر چندجمله‌ای f موجود است که $IS_2^1 \vdash \forall \vec{x}\ \varphi(\vec{x}, f(\vec{x}))$. این‌دو، IS_2^1 را نامزد خوبی برای معرفی شدن به‌عنوان یک نظریهٔ محاسبه‌پذیر عملی (feasible) می‌دانند، یعنی نظریه‌ای که دقیقاً چیزهایی را ثابت کند که دارای اثبات‌های کوتاه (چندجمله‌ای) باشند. در [M2] نشان داده شده است که نظریه های حساب محدود شهودی بنا شده بر استقراء چند جمله ای روی فرمولهای مرتبط با رده های P و NP، بر خلاف نظایر کلاسیک آنها، متمایز هستند. و. هارنیک[۲۲] [H]، نظریه‌های شهودگرایانهٔ نظیر S_2^i، $i \geq 1$، را نیز مطالعه کرده و نتایج مشابهی در مورد توابع به‌طور اثبات‌پذیر تام آن‌ها به‌دست آورده است.

تشکر

از آقای دکتر مجتبی آقایی به خاطر تلاش فراوان در برگزاری موفقیت آمیز کارگاه منطق در دانشگاه صنعتی اصفهان (جائیکه این مقاله اولین بار در آنجا ارائه شد) و آقای مصطفی زارع به خاطر کمک در تهیهٔ نسخهٔ نهایی تشکر فراوان دارم.

مراجع

[**BK**] A. Bovikin and R. Kaye, Order-Types of Models of Peano Arithmetic, Logic and Algebra, 275–285, Contemp. Math., 302, Amer. Math. Soc., Providence, RI, 2002 .

---

[۲۱] Urquhart
[۲۲] Harnik

[**Bur**] W. Burr, Fragments of Heyting Arithmetic, J. Symbolic Logic 63 (2000), 1223-1240.

[**Bus1**] S. Buss, Bounded Arithmetic, Bibliopolis, Napoli, 1986. Revision of 1985 Princeton University Ph.D. thesis.

[**Bus2**] S. Buss, Bounded Arithmetic and Propositional Proof Complexity. Logic of Computation (Marktoberdorf, 1995), 67-121, NATO Adv. Sci. Inst. Ser. F Comput. Systems Sci., 157, Springer, Berlin, 1997.

[**Bus3**] S. Buss, First Order Proof Theory of Arithmetic, in Hand Book of Proof Theory, ed. S. Buss, Elsevier Science, 1998.

[**Bus4**] S. Buss, Bounded Arithmetic, Proof Complexity and Two Papers of Parikh, Ann. Pure App. Logic, 96 (1999)43-55.

[**C**] S. A. Cook, The P versus NP Problem, available at http://www.cs.toronto.edu/ sacook/.

[**CU**] S. A. Cook and A. Urqhuart, Functional Interpretations of Feasibly Constructive Arithmetic, Ann. Pure and Appl. logic 63 (1993), 103-200.

[**D**] C. Dimitracopolos, On End Extensions of Models of Subsystems of Peano Arithmetic, Theo. Computer Sci., 257 (2001) 79-84.

[**H**] V. Harnik, Provably Total Functions of Intuitionistic Bounded Arithmetic, J. Symbolic Logic, 57 (1992) 466-477.

[**HP**] P. Hajek and P. Pudlak, Metamathematics of First-Order Arithmetic, Springer, 1993.

[**K1**] R. Kaye, Model-Theoretic Properties Characterizing Peano Arithmetic, J. Symbolic Logic, 56 (1991) 949-963.

[**K2**] R. Kaye, Models of Peano Arithmetic, Oxford University Press, Oxford, 1991.

[**Kr**] J. Krajicek, Bounded Arithmetic, Propositional Logic, and Complexity Theory, Cambridge University Press, 1995.

[**MM**] A. Macintyre and D. Marker, Primes and Their Residue Rings in Models of Open Induction, Ann. Pure Appl. Logic, 43 (1989) 57-77.

[**M**] Moj. Moniri, Recursive Models of Open Induction of Prescribed Finite Transcendence Degree > 1 with Cofinal Twin Primes, C. R. Acad. Paris Ser. I Mathe. 319 (1994) 903-908.

[**MOMO**] Mor. Moniri and Moj. Moniri, Some Weak Fragments of HA and Certain Closure Properties, J. Symbolic Logic, 67 (2002) 91-103.

[**M1**] Mor. Moniri, Intuitionistic Weak Arithmetic, Arch. Math. Logic, 42 (2003) 791-796.

[**M2**] Mor. Moniri, Comparing Constructive Arithmetical Theories Based on NP-PIND and coNP-PIND, J. Logic and Computation, 13 (2003) 881-888.

[**PH**] J. Paris and L. Harington, A Mathematical Incompleteness in Peano Arithmetic, in Hand Book of Mathematical Logic, ed. J. Barwise, North-Holland, 1977.

[**TD**] A. S. Troelstra and D. van Dalen, Constructivism in Mathematics, Vol. I, North-Holland, Amsterdam, 1988.

[**We**] K. F. Wehmeier, Fragments of HA Based on Σ_1-Induction, Arch. Math. Logic 37 (1997), 37-49.

[**Wilk**] A. J. Wilkie, Some Results and Problems on Weak Systems of Arithmetic, Logic Colloquium' 77, North-Holland, 1978, 285-296.

[**Wilm**] G. Wilmers, Bounded Existential Induction, J. Symbolic logic 40 (1985), 72-90.

[**WP**] A. Wilkie and J. Paris, On the Scheme of Induction for Bounded Arithmetic Formulas, Ann. Pure Appl, Logic 35 (1978) 261-302.