Research in Logic, Institute for Humanities and Cultural Studies (IHCS)
Biannual Journal, Vol. 12, No. 2, Autumn and Winter 2021-2022, 193-211
Doi: 10.30465/lsj.2021.36251.1358

Bounded Model Theory and its Applications to Bounded Arithmetic

Abolfazl Alam[*]

Morteza Moniri[**]

Abstract

Bounded model theory can be considered as part of first-order model theory, which its aim is to study model-theoretic notions in a language consisting of an order relation where all quantifiers are restricted to the bounded ones. One can apply bounded model theory to study some problems in bounded arithmetic. Bounded arithmetic can be considered as a sub-theory of first-order Peano arithmetic in an extended language. Bounded arithmetic has some applications in computational complexity theory. There are already some related bounded model-theoretic concepts like bounded quantifier elimination and bounded model completeness which has been applied to bounded arithmetic and complexity theory. In this article, we review some known results and prove some new ones in bounded model theory and use them to obtain certain results in bounded arithmetic and complexity theory. In particular, we define the notion of bounded model companion and study its relations to some fundamental problems in complexity theory.

Keywords: Bounded Arithmetic, Bounded formula, Bounded model complete, Bounded model companion, Bounded quantifier elimination.

* PhD Student, Department of Mathematics, Shahid Beheshti University, Tehran, Iran, abolfazlalam1989@gmail.com

** Faculty member, Department of Mathematics, Shahid Beheshti University (Corresponding Authour), ezmoniri@gmail.com

Date received: 18/04/2021, Date of acceptance: 19/07/2021

منطق‌پژوهی، پژوهشگاه علوم انسانی و مطالعات فرهنگی
دوفصل‌نامهٔ علمی (مقالهٔ علمی ـ مروری)، سال ۱۲، شمارهٔ ۲، پاییز و زمستان ۱۴۰۰، ۱۹۵ - ۲۱۱

نظریهٔ مدل محدود و برخی کاربردهای آن در حساب محدود

ابوالفضل علم*

مرتضی منیری**

چکیده

نظریهٔ مدل محدود را می‌توان بخشی از نظریهٔ مدل دانست که هدف آن بررسی مفاهیم و نتایج نظریهٔ مدل در یک زبان شامل یک رابطهٔ ترتیبی است در حالتی که سورهای موردبحث همگی از نوع محدود هستند. از نظریهٔ مدل محدود می‌توان برای مطالعهٔ مسائل مربوط به نظریهٔ حساب محدود استفاده کرد. حساب محدود را می‌توان زیرنظریه‌ای از حساب مرتبهٔ اول پئانو در زبانی گسترش‌یافته دانست. خود حساب محدود، کاربردهای فراوانی در نظریهٔ پیچیدگی محاسبات دارد. با تعریف و مطالعهٔ مفاهیم پایه‌ای نظریهٔ مدل در حالت محدود مانند حذف سور محدود و مدل کامل محدود، نتایج جالبی در نظریهٔ مدل با کاربردهایی در نظریهٔ پیچیدگی محاسبه و حساب محدود به دست آمده است. در این مقاله، ضمن مروری بر نتایج موجود در این زمینه، برخی مفاهیم و نتایج جدید را در این راستا ارائه می‌کنیم و ارتباط‌های آن‌ها را با برخی مسائل بنیادی در نظریهٔ پیچیدگی محاسبه مطالعه می‌کنیم.

کلیدواژه‌ها: حساب محدود، فرمول محدود، مدل کامل محدود، مدل همراه محدود، حذف سور محدود.

* دانشجوی دکتری، گروه ریاضی، دانشگاه شهیدبهشتی، تهران، ایران، abolfazlalam1989@gmail.com
** عضو هیئت علمی، گروه ریاضی، دانشگاه شهید بهشتی (نویسندهٔ مسئول)، ezmoniri@gmail.com
تاریخ دریافت: ۱۴۰۰/۰۲/۳۰، تاریخ پذیرش: ۱۴۰۰/۰۵/۲۶

۱. مقدمه

حساب مرتبهٔ اول محدود زیرنظریه‌ای از حساب مرتبهٔ اول پئانو است که با محدود کردن اصل استقرا به فرمول‌های محدود به دست می‌آید. فرمول‌های محدود فرمول‌های مرتبهٔ اولی در زبان حساب هستند که سورهای آنها همگی محدود (کراندار) هستند. اولین پژوهشی که به مطالعهٔ این دستگاه منطقی حساب پرداخت، توسط پریخ انجام گردید. ایشان در دو مقالهٔ (Parikh, 1971) و (Parikh, 1973) حساب مرتبهٔ اول محدود را معرفی و بررسی کرد. مهمترین قضیه‌ای که پریخ دربارهٔ حساب محدود ثابت کرد، بیان می‌کند هر تابعی که به طور اثبات‌پذیر تام باشد، از درجهٔ رشد حداکثر چندجمله‌ای برخوردار خواهد بود. به این دلیل، پریخ حساب محدود را نوعی حساب ملموس و از این نظر از حساب مرتبهٔ اول پئانو که تابع نمایی در آن به طور اثبات‌پذیر تام است، برتر می‌دانست.

ساموئل باس در سال ۱۹۸۶ و در رسالهٔ دکتری خود، زبانی جدید برای حساب محدود معرفی کرد و به بررسی رده‌هایی از زیر نظریه‌های این حساب پرداخت. اودر کار خود از اصلی ضعیف‌تر از اصلی که تام بودن تابع نمایی را بیان می‌کند، استفاده کرد و نشان داد که همین اصل ضعیف، مثلاً برای کدگذاری فرمول‌های حسابی و بیان و اثبات قضیهٔ ناتمامیت گودل برای نظریه‌هایش، کفایت می‌کند. باس، کوک و اورکهارت همچنین حساب‌های محدود متکی بر منطق شهودی را مطالعه کرده‌اند. برای مثال، منابع زیر را می‌توان دید:

(Buss, 1986, Buss, 1995, Buss, 1998, Cook 1975, Cook and Urquhart, 1993)

پژوهش باس و دیگرانی که کارهای او را دنبال کرده‌اند، مبتنی بر نظریهٔ برهان است و از روش‌های معنایی (نظریهٔ مدلی) کمتر استفاده کرده‌اند. مرتضی منیری در (Moniri, 2007) و (Moniri, 2006)به مطالعهٔ حساب محدود کلاسیک و شهودی با استفاده از نظریهٔ مدل پرداخت. با ادامه‌ی این مسیر، در این مقاله با استفاده از نظریهٔ مدل، به مطالعهٔ نظریهٔ حساب محدود خواهیم پرداخت.

پرسش بنیادی در نظریهٔ حساب محدود، این است که آیا این نظریه (یا زیرنظریه‌های آن) به طور متناهی اصل‌بندی می‌شوند یا خیر؟ این پرسش ارتباط مستقیمی با پرسش فروپاشی سلسله مراتب چندجمله‌ای از دید زمان در یک مدل از نظریهٔ مورد بحث دارد. درواقع، چون ردهٔ فرمول‌های Σ_i^b ردهٔ متناظر با ردهٔ محمولات Σ_i^p (محمولات محاسبه‌پذیر در زمان چندجمله‌ای (Krajicek, 1995)) است، فروریختن سلسله مراتب فرمول‌های محدود

معادل با فروپاشی PH است. پس این مسئله (فروپاشی سلسله مراتب فرمول‌های محدود) در حالت $i=1$، همان مسئلهٔ $NP=?coNP$ در مدل یا نظریهٔ مورد بحث است. بنابراین سوال اساسی این است که در کدام زیرنظریهٔ ضعیف حساب محدود (و یا کدام مدل از این نظریه‌ها) فرمول‌های Σ_1^b دارای معادل Π_1^b هستند. حالت خاص این مسئله، فروپاشی این فرمول‌ها در مدل استاندارد است، که در واقع همان مسئلهٔ بنیادی $NP=?coNP$ است.

مرتضی منیری در (Moniri, 2007) به مطالعهٔ این مسئله از دیدگاه نظریهٔ مدل پرداخت. او مفهوم مدل کامل محدود را برای مطالعهٔ این مسئله به کار گرفت. یک نظریه مانند T مدل کامل است اگر و تنها اگر برای هر دو مدل $M \subseteq N$ از T داشته باشیم $M \prec N$. T را مدل کامل محدود گوییم هرگاه T ، $M \subseteq N$ نتیجه دهد $M \prec^{\Sigma_1^b} N$. در این‌جا $M \subseteq N$ یعنی M زیر مدلی از N است و $M \prec N$ یعنی M زیر مدلی مقدماتی از N است. همچنین $M \prec^{\Sigma_1^b} N$ به این معنی است که M زیر مدلی از N است و هر فرمول Σ_1^b با پارامتر در M، در N درست است اگر و تنها اگر در M درست باشد. این تعریف جدید، منجر به گسترش برخی قضایای مهم در نظریهٔ مدل به حالت محدود، و در نتیجهٔ آن پیوند خوردن این بخش از نظریهٔ مدل با نظریهٔ مدل حساب محدود شد. در این مقاله، در فصل دوم، به بیان مفاهیم مقدماتی نظریهٔ مدل محدود و مرور نتایج به‌دست‌آمده در این حوزه می‌پردازیم. در فصل سوم، در دنبالهٔ مطالعات نظریه‌های مدل کامل محدود، مفهوم مدل همراه محدود را بیان نموده و ویژگی‌های آن را بررسی می‌کنیم. در فصل چهارم به ارتباط بین نظریهٔ مدل محدود و مفهوم مدل همراه محدود و مسائل اصلی نظریهٔ پیچیدگی از منظر برخی نظریه‌های ضعیف حساب محدود می‌پردازیم.

۲. پیش‌نیازها

در این فصل، در ابتدا مفاهیم ابتدایی نظریهٔ مدل محدود و حساب محدود را بیان می‌کنیم. فرض کنید L یک زبان مرتبهٔ اول شامل یک نماد محمولی دو موضعی $\leq$ باشد. در سرتاسر این مقاله، منظور از یک نظریه که به صراحت مشخص نشده است، یک نظریه در زبان L است که در آن $\leq$ خواص ترتیب‌های جزئی را دارد.

در یک فرمول، یک سور را محدود گوییم هرگاه به شکل $\forall x \leq t(\overline{y})$ و یا $\exists x \leq t(\overline{y})$ ظاهر شود که در آن x یک متغیر و $\overline{y}$ دنباله‌ای متناهی از متغیرها باشد

که x در آن حضور ندارد. فرض کنید t یک ترم و $\varphi(x)$ یک فرمول در زبان L باشد. منظور از فرمول $\forall x \leq t\varphi(x)$، فرمول $\forall x\ (x \leq t \rightarrow \varphi(x))$ و منظور از $\exists x \leq t\varphi(x)$ فرمول $\exists x\ (x \leq t \wedge \varphi(x))$ است. گوییم $\varphi(\overline{x})$ یک فرمول محدوداست، هرگاه همهٔ سورهای بکار رفته در آن محدود باشند. همچنین گوییم نظریهٔ T یک نظریهٔ محدود است، هرگاه بوسیلهٔ مجموعه‌ای از فرمول‌های محدود اصل‌پذیر باشد.

گوییم نظریهٔ T به طور محدود کامل است، هرگاه برای هر جملهٔ محدود مانند σ، داشته باشیم T گσ یا T گ$\neg\sigma$. همچنین، یادآوری می‌نماییم که منظور از دیاگرام مدل M، مجموعهٔ همهٔ فرمول‌های $\varphi(\overline{a})$ در زبان گسترش یافتهٔ $L \cup M$ است جایی که $\overline{a} \in M$ و $\varphi(\overline{a})$ ، M. دیاگرام M را با $Diag(M)$ نشان می‌دهیم.

۱.۲ زبان حساب محدود

زبان مرتبهٔ اول حساب محدود معرفی شده توسط باس، شامل نمادهای تابعی $S,\ 0,\ +,\ \times,\ |x|,\ \left\lfloor \frac{1}{2}x \right\rfloor,\ \#$ و نماد محمولی $\leq$ است. تعبیر نمادهای $\times,\ +,\ 0$ در مدل استاندارد به شکل معمول است. نماد S به صورت $S(n) = n+1$ تعبیر می‌شود. برای عدد طبیعی x، $|x|$ برابر با تعداد ارقام نمایش دودویی x و $\left\lfloor \frac{1}{2}x \right\rfloor$ برابر با بزرگترین عدد طبیعی که از $\frac{x}{2}$ کمتر یا مساوی است تعبیر می‌شود. همچنین برای هر x, y داریم $\#(x,y) = 2^{|x|\cdot|y|}$. نکتهٔ قابل توجه در مورد این زبان این است که تمام اعداد طبیعی بوسیله ترم‌های زبان قابل بیان هستند.

تعریف۱فرض کنید $t(x)$ یک ترم و φ یک فرمول در زبان حساب محدود باشد. در این‌صورت به فرمول‌های φ و $\forall x \leq |t(\overline{y})|\varphi$ فرمول‌های شدیداً محدود گفته می‌شود.

اکنون رده‌بندی فرمول‌های محدود براساس پیچیدگی را بیان می‌کنیم. فرض کنید Δ_0^b مجموعهٔ همهٔ فرمول‌های شدیداً محدود (شامل فرمول‌های بدون سور) باشد. دنباله‌های $\{\Sigma_i^b\}_{i\in\omega}$ و $\{\Pi_i^b\}_{i\in\omega}$ به صورت بازگشتی تعریف می‌شوند:

$$\Sigma_0^b = \Pi_0^b = \Delta_0^b \text{ـ}۱،$$

۲- برای هر عدد طبیعی i داریم $\Sigma_i^b, \Pi_i^b \subseteq \Pi_{i+1}^b$ و $\Sigma_i^b, \Pi_i^b \subseteq \Sigma_{i+1}^b$،

۳- اگر φ فرمولی در Π_{i+1}^b و $t(\overline{y})$ یک ترم زبان باشد، آنگاه $\forall x \leq t(\overline{y})\varphi$ و $\exists x \leq \left|t(\overline{y})\right|\varphi$ نیز عضوهایی از Π_{i+1}^b هستند.

۴- اگر φ فرمولی در Σ_{i+1}^b و $t(\overline{y})$ یک ترم زبان باشد، آنگاه $\exists x \leq t(\overline{y})\varphi$ و $\forall x \leq \left|t(\overline{y})\right|\varphi$ نیز عضوهایی از Σ_{i+1}^b هستند.

۵- اگر $\varphi \in \Sigma_i^b$ و $\psi \in \Pi_i^b$ آنگاه $\neg\varphi \in \Pi_i^b$ و $\neg\psi \in \Sigma_i^b$.

۶- دو مجموعه Σ_{i+1}^b و Π_{i+1}^b تحت ترکیب فصلی و عطفی بسته هستند.

در (منیری، ۱۳۸۴) خلاصه‌ای از تعاریف و نتایج اساسی مربوط به حساب محدود شرح داده شده است. در اینجا به اندکی از قضایای مهم آن بسنده می‌کنیم.یکی از اساسی‌ترین و مهم‌ترین نتایجی که در مورد نظریه‌های محدود وجود دارد، قضیهٔ زیر از پریخ است.

قضیهٔ ۲ فرض کنید φ یک فرمول محدود و T یک نظریهٔ محدود باشد. اگر $T \vdash \forall\overline{x}\ \exists y\ \varphi$، آنگاه ترم t در زبان L وجود دارد به طوریکه $T \vdash \forall\overline{x}\ \exists y \leq t\varphi$.

قضیهٔ ۳ برای هر $i \geq 1$، زیرمجموعهٔ A از اعداد طبیعی به رده‌ی پیچیدگی Σ_i^p متعلق است اگر و تنها اگر فرمولی در Σ_i^b موجود باشد که زیرمجموعه‌ای از $\square$ که به‌وسیله‌ی آن تعریف می‌شود، برابر با A باشد.

این قضیه نشان می‌دهد فروپاشی سلسله مراتب فرمول‌های محدود معادل با فروپاشی PH (سلسله مراتب زمان چندجمله‌ای) است. بنابراین فروپاشی سلسله مراتب فرمول‌های محدود از اهمیت ویژه‌ای برخوردار است. بررسی فروپاشی PH در زیرنظریه‌های حساب و مدل‌های آن‌ها نیز مسئله‌ای مورد توجه پژوهشگران است. در ادامه برخی از زیرنظریه‌های شناخته شدهٔ حساب محدود را معرفی می‌کنیم.

۲.۲ نظریه‌های S_2^i و T_2^i

$BASIC$ مجموعه‌ای از ۳۲ اصل است که خواص پایه‌ای نمادهای زبان حساب محدود را بیان می‌کنند.برای نمونه، می‌توان به دو اصل $\forall x, y\ (x \leq y \rightarrow x < s(y))$ و $\forall x\ (x \neq s(x))$ اشاره نمود. برای دیدن لیست کامل جملات $BASIC$ می‌توانید به

(Krajicek, 1995) و (Buss, 1986) مراجعه کنید. در اینجا به معرفی چند اصل مرتبط با استقرا می‌پردازیم.

فرض کنید Ψ مجموعه‌ای از فرمول‌ها باشد. مجموعهٔ اصول $\Psi - IND$ به صورت

$$\left[\varphi(0) \wedge \forall x\ (\varphi(x) \to \varphi(s(x)))\right] \to \forall x\ \varphi(x)$$

تعریف می‌شود کهدر آن $\varphi \in \Psi$.

هم‌چنین مجموعهٔ $\Psi - PIND$ نیز به شکل

$$\left[\varphi(0) \wedge \forall x\ \left(\varphi(\left\lfloor \frac{1}{2}x \right\rfloor) \to \varphi(x)\right)\right] \to \forall x\ \varphi(x)$$

تعریف می‌شود که در آن $\varphi \in \Psi$.

تعریف ۴نظریه‌های حساب محدود به شکل زیر تعریف می‌شوند. فرض کنید i عددی طبیعی باشد.

۱. مجموعهٔ اصول نظریهٔ S_2^i برابر است با $BASIC \cup \Sigma_i^b - PIND$.

۲. مجموعهٔ اصول نظریهٔ T_2^iبرابر است با $BASIC \cup \Sigma_i^b - IND$.

۳. $S_2 = \bigcup_{i<\omega} S_2^i$.

۳. $T_2 = \bigcup_{i<\omega} T_2^i$.

بنابر یک نتیجهٔ مشهور، برای هر i، داریم $S_2^i \subseteq T_2^i \subseteq S_2^{i+1}$ و در نتیجه $S_2 = T_2$. یک پرسش باز حساب محدود این است که آیا شمول در دنبالهٔ

$$S_2^1 \subseteq S_2^2 \subseteq \ldots$$

اکید است یا خیر؟ یعنی آیا $i > 0$ وجود دارد که $S_2^i = S_2^{i+1}$؟

قضیهٔ ۵اگر PH فرو نریزد، آنگاه شمول در دنبالهٔ $S_2^1 \subseteq S_2^2 \subseteq \ldots$ اکید است. هم‌چنین، این شمول اکید است اگر و تنها اگر S_2 به طور متناهی اصل‌بندی شود.

این قضیه، اهمیت نظریه‌های حساب محدود را نشان می‌دهد. مهم‌ترین نظریه در این میان S_2^1 است. ما نیز در این مقاله تمرکز را بر مطالعه روی S_2^1 قرار داده‌ایم. نظریهٔ دیگری از حساب محدود که مرتبط با S_2^1 بوده و مورد توجه پژوهشگران است، PV نام دارد. در ادامه به معرفی این نظریه می‌پردازیم.

۳.۲ نظریه‌های PV و CPV

نظریهٔ PV اولین بار توسط کوک معرفی شد. PV اصالتاً نظریه‌ای معادلاتی (equational theory) است که زبان آن شامل نمادهای تابعی برای توابع محاسبه‌پذیر در زمان چندجمله‌ای است و اصول آن تعریف این توابع را به دست می‌دهند. اما معمولاً گسترش PV به منطق مرتبهٔ اول را نیز با همین نماد نشان می‌دهند. این نظریه و S_2^1، نتایج جهانی یکسانی دارند. نتیجهٔ زیر از باس، (Buss, 1986)، برای ما اهمیت دارد.

گزارهٔ ۶فرض کنید T گسترشی سازگار از PV و $\varphi(x)$ فرمولی Σ_1^bیا Π_1^b باشد. اگر T گ$\forall x\varphi(x)$، آنگاه $\forall x\varphi(x)$ ‘ □.

برهان. فرض کنید عدد طبیعی n موجود باشد به طوریکه $\neg\varphi(n)$ ‘ □. در این‌صورت $\neg\varphi(n)$گ-S_2^1. در حالتی که φفرمولی Σ_1^b باشد، $\neg\varphi$ فرمولی جهانی است. چون PV و S_2^1 نتایج جهانی یکسانی دارند، $\neg\varphi(n)$گ-PV. در حالتی که φ فرمولی Π_1^b باشد، $\neg\varphi$ یک فرمول Σ_1^b است. می‌دانیم PV و S_2^1 در مورد فرمول‌های $\forall\Sigma_1^b$ توافق دارند. بنابراین $\neg\varphi(n)$گ-PV. این با فرض در تناقض است. منظور از CPVنظریه‌ای است که از گسترش طبیعی نظریهٔ S_2^1به زبان PV حاصل می‌شود. CPV گسترشیمحافظه‌کارانه ازPVاست(Cook, Urquhart, 1993).

۳. نظریهٔ مدل محدود

همان‌طور که قبلا گفته شد، در (Moniri, 2007) مفاهیمی از نظریهٔ مدل به حالت محدود گسترش داده شد و از آن برای نشان دادن نتایجی در حساب محدود بهره گرفته شد. در این‌جا برخی از این مفاهیم را مرور می‌کنیم. فرض کنید $M \subseteq N$ دو مدل در زبان L باشند. گوییم M به طور Σ_i^b در N می‌نشیند و می‌نویسیم $M \prec^{\Sigma_i^b} N$ هرگاه برای

هر فرمول $\varphi(x)$ در Σ_i^b و هر $b \in M$، اگر $M \models \varphi(b)$، آنگاه $N \models \varphi(b)$. به مدل M یک مدل بطور وجودی بستهٔ Σ_i^b از نظریهٔ T گوییم هرگاه برای هر $N \models T$ که $M \subseteq N$ داشته باشیم $M \prec^{\Sigma_i^b} N$. M بطور وجودی بستهٔ محدود است هرگاه به طور وجودی بستهٔ Σ_1^b باشد. نظریهٔ T دارای خاصیت مدل کامل محدود (bounded model complete) است هرگاه برای هر دو مدل $M \subseteq N$ از T داشته باشیم $M \prec^{\Sigma_i^b} N$ (درواقع هر مدل از آن مدلی وجودی بستهٔ Σ_1^b باشد). این خاصیت یک تعمیم ازنسخهٔ کلاسیک خود است. حساب مرتبهٔ اول پئانو PA مثال ساده‌ای از یک نظریه است که به وضوح مدل کامل محدود است اما مدل کامل نیست. اینکه کدام نظریهٔ حساب محدود مدل کامل محدود است (یا نیست) مسئله‌ای جالب توجه است که در بخش‌های بعدی به آن خواهیم پرداخت.

۱.۳ چند نتیجهٔ پایه‌ای

در این بخش، چند نتیجهٔ از قبل دانسته در مورد مفاهیم مطرح‌شده را بیان می‌کنیم (Moniri, 2007:46).

قضیهٔ ۷ فرض کنید T یک نظریهٔ محدود باشد. در اینصورت شرایط زیر با هم معادل هستند.

۱. نظریهٔ T مدل کامل محدود است.

۲. هر مدل T مدلی به طور وجودی بستهٔ محدود از T است.

۳. برای هر Σ_1^b-فرمول مانند $\varphi(\overline{x})$، فرمول $\psi(\overline{x})$ در Π_1^b وجود دارد به طوری که T گ$\forall \overline{x}(\varphi(\overline{x}) \leftrightarrow \psi(\overline{x}))$.

۴. برای هر فرمول محدود مانند $\varphi(\overline{x})$، فرمول $\psi(\overline{x})$ در Π_1^b وجود دارد به طوری که T گ$\forall \overline{x}(\varphi(\overline{x}) \leftrightarrow \psi(\overline{x}))$

این قضیه به نوعی بیان کننده این مطلب است که مدل کامل محدود بودن یک نظریه معادل با فروریختن سلسله مراتب فرمول‌های محدود(و در نتیجه فرو ریختن PH) در آن نظریه است. بنابراین، مسئلهٔ مورد علاقه این است که تحت چه شرایطی، نظریه‌های S_2^i مدل کامل محدودند.

یکی از نتایج قضیهٔ۷ این است کـه اگـر نظریـهٔ T یـک نظریـهٔ محـدود و مـدل کامـل محدود باشد آنگاه می‌توان T را بوسیلهٔ فرمول‌های $\forall\Sigma_1^b$ اصل‌بندی نمود. این نیز منجربـه نتیجهٔ جالب زیر در مورد برابر بودن دو نظریهٔ حسابی S_2^1 و PV می‌گردد.

نتیجـهٔ ۸ اگـر S_2^1 و PV برابـر نباشـند، آنگـاه S_2^1 دو مـدل ماننـد $M \subseteq N$ دارد که $M \prec^{\Sigma_1^b} N$ برقرارنیست.

در ادامه این بخش به معرفی مفهوم دیگری از نظریهٔ مدل محدود، به نـام حـذف سـور محدود می‌پردازیم. گوییم نظریهٔ T حذف سـور محـدود(bounded quantifier elimination) دارد هرگاه هر فرمول محدود معادلی بدون سور در Tداشته باشد. به راحتی با استقراء روی پیچیدگی فرمول می‌توان نشان داد که این تعریف معـادل ایـن اسـت کـه هـر فرمـول Σ_1^b معادلی بدون سور در Tداشته باشد.

۲.۳ مدل همراه محدود

در نظریهٔ مدل، نظریه‌هایی هستند که مدل کامل نیستند. برای این نظریه‌ها مفهـومی بـه نـام مدل همراه تعریف می‌شود. مدل همراه یک نظریه، نظریهٔ دیگری است که مدل کامل بـوده و دارای نتایج جهانی یکسانی با نظریهٔ اولیه است. در واقع، اگـر T یـک نظریـه باشـد، بـه نظریهٔ مدل کامل U، مدل همراه نظریهٔ T گوییم هرگاه برای هر جملـه عمـومی ماننـد σ داشته باشیم σگ T اگر و تنهـا اگـر σگ U. اکنـون ایـن مفهـوم را در حالـت محـدود تعریف می‌کنیم. در بخش‌های بعد (به ویژه ۱.۴) با برخی از کاربردهای این مفهـوم مواجـه خواهیم شد.

تعریف ۹ فرض کنید T یک نظریه باشد. فرض کنید U یک نظریهٔ سازگار محـدود و مدل کامل محدود باشد. نظریهٔ U را مـدل همـراه محـدود (bounded model companion) نظریهٔ T گوییم هرگاه هر دو نظریه روی جملات جهانی توافق داشته باشند.

قضیهٔ ۱۰فرض کنید T یـک نظریـهٔ $\forall\Sigma_1^b$ و U نظریـهٔ مـدل همـراه محـدودی بـرای T باشد. در اینصورت M ، U اگر و تنها اگر M مدلی به طور وجـودی بسـته محـدود برای T باشد.

برهان.فرض کنیـد M مـدلی از U باشـد. بنـابر تعریـف، M در مـدلی از T ماننـد N می‌نشیند و N نیز در مدلی از U مانند K می‌نشـیند (زیـرا U و T نتـایج جهـانی

یک‌سانی دارند). چون M مدلی وجودی بستهٔ محدود U است پس $M \prec^{\Sigma_1^b} K$ و درنتیجه $M \prec^{\Sigma_1^b} N$. این نیز نتیجه می‌دهد M ، T، چون T یک نظریهٔ $\forall\Sigma_1^b$ است. هم‌چنین اگر $M \subseteq M'$ و T ، M' آنگاه بوسیلهٔ استدلال مشابه می‌توان ثابت نمود $M \prec^{\Sigma_1^b} M'$. پس M مدل به طور وجودی بستهٔ محدود از نظریهٔ T است.

به عکس. فرض کنید Mمدلی به طور وجودی بستهٔ محدود از T باشد. در این صورت N ، U و K ، T وجود دارند که $M \subseteq N \subseteq K$. چون M وجودی بستهٔ محدود است، $M \prec^{\Sigma_1^b} K$ و چون N مدل U است، $N \prec^{\Sigma_1^b} K$. این نیز نتیجه می‌دهد $M \prec^{\Sigma_1^b} N$. پس M ، U. ■

در نظریهٔ مدل، اگر زنجیری از زیرمدل‌های مقدماتی وجود داشته باشد، آنگاه هر مدل از زنجیر در اجتماع زنجیر به طور مقدماتی می‌نشیند. نسخهٔ محدود از این قضیه، که به قضیهٔ زنجیر مقدماتی مشهور است، در کتاب (Chang and Keisler, 1990) بیان شده است.

قضیهٔ ۱۱ (قضیه زنجیر Σ_1^b-مقدماتی) فرض کنید $\{M_i\}_{i<\lambda}$ یک زنجیر از مدل‌ها باشد که برای هر $i < j$، داشته باشیم $M_i \prec^{\Sigma_1^b} M_j$. در اینصورت برای هر $k < \lambda$ خواهیم داشت $M_k \prec^{\Sigma_1^b} M = \bigcup_{j<\lambda} M_j$.

برهان. فرض کنید M ، $\exists x \le t\varphi(x,b)$ که $b \in M_k$. در اینصورت $a \in M$ وجود دارد که M ، $a \le t \wedge \varphi(a,b)$. فرض کنید $a \in M_l$ که $k < l$. در این‌صورت M_l ، $a \le t \wedge \varphi(a,b)$ و در نتیجه M_l ، $\exists x \le t\varphi(x,b)$. چون $M_k \prec^{\Sigma_1^b} M_l$ داریم M_k ، $\exists x \le t\varphi(x,b)$. ■

از این قضیه در اثبات یکتایی نظریهٔ مدل همراه محدود استفاده می‌شود.

نتیجهٔ ۱۲اگر T یک نظریهٔ $\forall\Sigma_1^b$ باشد که مدل همراه محدود دارد، آنگاه نظریهٔ مدل همراه محدود آن در حد هم‌ارزی یکتاست.

برهان. فرض کنید T' و T'' دو نظریهٔ مدل همراه محدود برای T باشند. در این‌صورت T' و T'' دو نظریهٔ مدل کامل محدود و دارای نتایج جهانی یکسان هستند. بنابراین زنجیر

$M_1 \subseteq M_2 \subseteq ...$

از مدل‌ها وجود دارد که برای هر عدد طبیعی k، T' ، M_{2k-1} و T'' ، M_{2k}. با استفاده از قضیهٔ زنجیر Σ_1^b – مقدماتی، اجتماع این مدل‌ها گسترشی Σ_1^b – مقدماتی از M_1 (و بنابر استدلالی مشابه، از M_2) است. در نتیجه T' ، M_1. بنابر استدلال مشابه می‌توان گفت هر مدل T'' یک مدل T' است. در نتیجه T'' و T'هم‌ارز هستند.■

در نظریهٔ مدل، وجود مدل همراه برای یک نظریه، معادل با اصل‌پذیر بودن ردهٔ همه مدل‌های وجودی بسته آن است. در حالت محدود نیز، این حکم برقرار است.

قضیهٔ ۱۳فرض کنید T یک نظریهٔ $\forall\Sigma_1^b$ باشد. در اینصورت T مدل همراه محدود دارد اگر و تنها اگر ردهٔ همهٔ مدل‌های وجودی بستهٔ محدود آن بوسیلهٔ یک نظریهٔ محدود اصل‌بندی گردد.

برهان. فرض کنید K ردهٔ همهٔ مدل‌های وجودی بستهٔ محدود T باشد. فرض کنید K به‌وسیلهٔ نظریهٔ محدود T'اصل‌بندی شود. هر مدل از T' مدلی از T است. همچنین هر مدل T در مدلی بطور وجودی بستهٔ محدود از T می‌نشیند. پس هر مدل از T در مدلی از T' می‌نشیند. پس T' و T نتایج جهانی یکسانی دارند. اکنون کافیست نشان دهیم T' مدل کامل محدود است. این نیز واضح است، زیرا هر نشاندن بین مدل‌های T' از جنس Σ_1^b – مقدماتی است. پس T مدل همراه محدود دارد. جهت دیگر قضیه، بنابر قضیهٔ ۱۰ واضح است.■

در ادامهٔ مطالعهٔ مفاهیم نظریهٔ مدل در حالت محدود، مفهوم مدل مکمل محدود را بررسی می‌کنیم.

تعریف ۱۴ گوییم نظریهٔ T' مدل مکمل محدود (bounded model completion) نظریهٔ T است هرگاه T' مدل همراه محدود T بوده و برای هر T ، M نظریهٔ $T' \cup Diag(M)$ یک نظریهٔ به طور محدود کامل باشد.

همان‌طور که مدل مکمل و حذف سور در نظریهٔ مدل مرتبط هستند، در حالت محدود نیز این دو مفهوم یکدیگر را نتیجه می‌دهند.

لم ۱۵نظریهٔ مدل کامل محدود T حذف سور محدود دارد اگر و تنها اگر T یک مدل مکمل محدود برای $T_\forall$ باشد.

برهان. فرض کنید T مدل مکملی محدود برای $T_\forall$باشد. فرض کنید $\varphi(\overline{x})$ یک فرمول محدود و $\Sigma(\overline{x})$ مجموعهٔ همهٔ نتایج بدون سور $T\cup\{\varphi(\overline{x})\}$ باشد. هم‌چنین فرض کنید برای T ، $\overline{a}\in M$ مدل M تایپ $\Sigma(\overline{a})$ را محقق کند. همچنین فرض کنید D نظریهٔ $Diag(M,\overline{a})$ باشد (که در زبان جدید $L\cup\{\overline{a}\}$ تعریف می‌شود). چون $T\cup D$ با $T\cup\Sigma(\overline{a})$ سازگار است، با $\varphi(\overline{a})$ نیز سازگار خواهد بود. از طرفی چون $T\cup D$ به طور محدود کامل است، $\varphi(\overline{a})$ ، $T\cup D$. بنابراین $(M,\overline{a})$ مدلی از $\varphi(\overline{a})$ خواهد بود. این نیز نتیجه می‌دهد φ ، $T\cup\Sigma$. بنابر فشردگی، $\psi\in\Sigma$ وجود دارد که T ، $\varphi\leftrightarrow\psi$. پس T حذف سور محدود دارد.

اکنون اگر نظریهٔ مدل کامل محدود T حذف سور محدود داشته باشد، کافیست برای مدل $T_\forall$ ، M نشان دهیم $T\cup Diag(M)$ به طور محدود کامل است. این نیز واضح است. زیرا هر فرمول محدود مانند φ با فرمولی بدون سور مانند ψ (در T) معادل است و بنابراین $T\cup Diag(M)$یکی از ψ یا $\neg\psi$ را ثابت می‌کند.■

۴. مدل همراه نظریه‌های ضعیف حساب

در این فصل، به مطالعهٔ شرایط لازم و یا کافی برای اینکه نظریه‌های ضعیف حساب، مدل همراه محدود داشته باشند می‌پردازیم. برای این کار ابتدا لازم است با مفهوم دستگاه‌های اثباتی در منطق گزاره‌ای آشنا شویم. فرض کنید $p_1,p_2,\ldots$ مجموعهٔ همهٔ‌اتم‌های زبان باشد. مجموعهٔ راستگوهای زبان را با $TAUT$ نشان می‌دهیم. یک دستگاه اثباتی را می‌توان تابعی محاسبه‌پذیر در زمان چندجمله‌ای چون P دانست به طوری که برد آن در $TAUT$ قرار دارد و برای هر راستگوی τو دنبالهٔ w از جملات، $P(w)=\tau$ به معنای آن است که wاثباتی برای τ، در دستگاه P است. به w یک P–اثبات برای τ گوییم. تعداد نمادهای بکار رفته در w را طول اثبات گفته و آن را با $|w|$ نشان می‌دهیم. گوییم دستگاه اثباتی P از طول چندجمله‌ای است هرگاه چندجمله‌ای $f(x)$ موجود باشد به‌طوری که برای هر راستگوی τ، طول اثبات τ در دستگاه P حداکثر $f(|\tau|)$ باشد. مسئلهٔ زیر یکی از مهمترین مسائل باز در منطق ریاضی است.

مسئله: آیا دستگاه اثباتی P موجود است که در آن هر راستگو اثباتی با طول چندجمله‌ای داشته باشد؟

استفن کوک نشان داد کـه وجـود چنـین دسـتگاهی معـادل بـا $NP = coNP$ اسـت (Cook,1975).

مسئلهٔ ساده‌تر، این است که در کدام دستگاه‌ها، همهٔ راستگوها اثبات دارنـد. دسـتگاهی اثباتی که چنین ویژگی را داشته باشد، یک دستگاه کامل گوییم. اما اثبات صوری کامل بودن یک دستگاه در یک نظریهٔ حساب محدود می‌تواند دشوار باشد. در برخی نظریه‌ها، سـختی این مسـئله بـه انـدازه‌ی مسـئلهٔ $NP = ?\, coNP$ اسـت. مثـالی از چنـین دسـتگاه‌هـایی، دستگاه‌های اثباتی فرگه و فرگه گسترش یافته هستند. منظور از یک دسـتگاه اثبـاتی فرگـه، یک دستگاه اصل‌موضوعی معمولی شامل مجموعه‌ای از اصول بـه همـراه مجموعـه‌ای از قواعد است. به طور مثال قاعدهٔ MP یک قاعدهٔ آشنا در این زمینـه اسـت. منظـور از یـک دستگاه اثباتی فرگه گسترش یافته (EF)، دستگاهی اثباتی از نوع فرگه است که در آن این امکـان وجـود دارد کـه در اثبـات‌هـا گـزاره‌هـای پیچیـده بـا فرمـول‌هـای اتمـی جدیـد جایگزین شوند. قضیهٔ مشهوری در این زمینه وجود دارد که بیان می‌کند در نظریه‌های S_2^1 و CPV سه گزارهٔ زیر معادل هستند (Krajicek, 1995):

۱- $P = NP$.

۲- $NP = coNP$.

۳- دستگاه EF کامل است.

۱.۴ نتایجی در باب دستگاه‌های اثباتی

اگر P یک دستگاه اثباتی فرگه و یا فرگه گسترش یافته باشد، فرمول $PRF_p(y,x)$ یـک فرمول حسابی بدون سور است که بیان می‌کند « y اثباتی برای x در P است». هـم‌چنـین فرمول $Taut(x)$، فرمولی Π_1^b است که بیـان مـی‌کنـد «x یـک راسـتگو اسـت». اکنـون فرض کنید $t(x)$ یک ترم باشد. فرمول

$$taut(x) \rightarrow \exists y \leq t(x) PRF_p(y,x)$$

یک فرمول Σ_1^b است که بیان می‌کند هر راستگو دارای اثبـاتی کوتـاه اسـت. در ادامـه، جملهٔ حسابی « EF محدود به t است» برای نشان دادن فرمول فـوق بـرای یـک دسـتگاه

اثباتی فرگه گسترش یافته دلخواه به کار می‌رود. این فرمول را با χ_t نمایش می‌دهیم. توجه کنید که بنابر نتیجه‌ای در نظریهٔ پیچیدگی اثبات‌ها، دستگاه‌های اثبات فرگه گسترش‌یافته با یک‌دیگر به طور چندجمله‌ای قابل شبیه سازی هستند. یعنی آن‌که اثباتی کوتاه در یکی، در زمان چندجمله‌ای قابل تبدیل به اثباتی کوتاه در دیگری است. به همین دلیل فرمول « EF محدود به t است» وابسته به دستگاه اثباتی نیست.

همان‌طور که گفتیم، دستگاه‌های فرگه نقشی مهم در نظریهٔ پیچیدگی دارند. ارتباطی که می‌توان بین این دستگاه‌های اثباتی و نظریهٔ مدل محدود یافت، به مفهوم مدل کامل بودن بی‌ربط نیست.

نتیجهٔ ۱۶مدل M از PV، مدلی به طور وجودی بستهٔ محدود از PV است، اگر و تنها اگر EF در M کامل باشد.

برهان.می‌دانیم مدل EF در PV ، M کامل است اگر و تنها اگر هر گسترش از آن Σ_1^b–مقدماتی باشد(Krajicek, 1995). اکنون، بنابر قضیهٔ ۱۳، نظریهٔ PV مدل همراه محدود دارد اگر و تنها اگر ردهٔ مدل‌های به طور وجودی بستهٔ محدود آن مقدماتی محدود باشد (بوسیلهٔ یک نظریهٔ محدود اصل‌بندی شود). ■

فرض کنید PV ، M. در اینصورت گوییم جملهٔ $NP = coNP$ در M برقرار است هرگاه هر فرمول Σ_1^b با پارامتر در M، معادلی Π_1^b در M (با پارامتر در M) داشته باشد. مسئلهٔ اصلی در اینجا، پرسش زیر است:

مسئله: آیا ردهٔ مدل‌های $PV + NP = coNP$ یک ردهٔ مقدماتی محدود است؟

این مقاله، پاسخی برای این پرسش ارائه نمی‌دهد، اما قصد داریم در ادامه، این مسئله را از جنبهٔ نظریهٔ مدل محدود بررسی نماییم. فرض کنید مدل M از PV و ترم $t(x)$ وجود داشته باشد که EF در M محدود به t باشد. در این صورت $PV + \chi_t$ نظریهٔ محدود و سازگاری است که (بنابر آنچه در بالا گفته شد) مدل کامل محدود است. آن‌چه باقی می‌ماند، این است که آیا دو نظریهٔ PV و $PV + \chi_t$ نتایج جهانی یکسانی دارند یا خیر. قضیه‌ای که در زیر بیان می‌شود، احتمال منفی بودن پاسخ مسئلهٔ فوق را تحکیم می‌بخشد.

قضیهٔ ۱۷اگر PV مدل همراه محدود داشته باشد، آنگاه $NP = coNP$ (در مدل استاندارد).

برهان. فرض کنید T یک نظریهٔ مدل همراه محدود برای PV باشد. چون PV یک نظریهٔ جهانی است پس $PV = T_{\forall}$ و این نیز نتیجه می‌دهد T گسترشی محدود سازگار از PV است. پس بنابر گزارهٔ۶ هر قضیه از آن در مدل استاندارد برقرار است. از طرفی T مدل کامل محدود است. پس Σ_1^b – فرمول $\varphi(x)$ وجود دارد که

T گ$\forall x(Taut(x) \leftrightarrow \varphi(x))$

در نتیجه این جمله در مدل استاندارد نیز برقرار است. این نتیجه می‌دهد $NP = coNP$. ■

۲.۴ مدل مکمل محدود در PV

در این بخش، کاربردی از مفهوم مدل مکمل محدود در نظریهٔ PV بیان می‌کنیم. همان‌طور که وجود مدل همراه محدود برای PV، شرطی قوی‌تر از مسئلهٔ اصلی نظریهٔ پیچیدگی است (قضیهٔ۱۷)، وجود مدل مکمل محدود نیز، شرطی قوی‌تر از دیگر مسئلهٔ اساسی در نظریهٔ پیچیدگی است. در واقع، اگر PV مدل مکمل محدود داشته باشد، مدل همراه محدود نیز دارد و این بنابر قضیه ۱۷، منجر به $NP = coNP$ می‌گردد. اما نمی‌توانیم از این مطلب استنتاج کنیم که $P = NP$. برای این کار کافی بود PV گ$NP = coNP$ اما این نامحتمل است.

گزارهٔ ۱۸اگر PV مدل مکمل محدود داشته باشد، آنگاه $P = NP$.

برهان. فرض کنید T مدل مکملی محدود برای PV باشد. بنابر لم ۱۵، نظریهٔ T حذف سور محدود دارد. بنابراین هر Σ_1^b – فرمول، هم‌ارزی بدون سور در Tدارد. این به آن معنی است که $P = NP$ گT. از طرفی دیاگرام مدل استاندارد (که در واقع همهٔ جملات بدون سور و درست در مدل استاندارد است) همراه با T یک نظریهٔ سازگار و به‌طور محدود کامل است. به راحتی می‌توان نشان داد که مدل استاندارد در M به‌طور Σ_1^b – مقدماتی می‌نشیند. پس $P = NP$ در مدل استاندارد برقرار است.■

۵. نتیجه‌گیری

در این مقاله، برخی از مفاهیم نظریهٔ مدل به عنوان بخشی از منطق ریاضی از قبیل حذف سور، مدل کامل بودن و مدل همراه داشتن را در زمینه‌ی حساب مرتبه‌ی اول محدود

بازتعریف کرده و خواص آن‌ها را مطالعه کرده‌ایم. از جمله دستاوردهای این مطالعه، یـافتن برخی شرط‌های منطقی می‌باشد که با بعضی از گـزاره‌هـای مشـهور در نظریـهٔ پیچیـدگی محاسبه که به عنوان سؤال باز مطرح هستند، هم‌ارز هستند.

کتاب‌نامه

منیری، مرتضی (۱۳۸۴). «نظریهٔ مرتبهٔ اول پئانو و زیرنظریه‌های آن همراه باچنـد مسـئلهٔ مـرتبط در نظریهٔ پیچیدگی»، فرهنگ و اندیشهٔ ریاضی، ۲۴، صص. ۳۳–۵۵.

Buss, S. R. (1986).Bounded Arithmetic, Napoli: Bibliopolis.

Buss,S. R .(1995). Relating the Bounded Arithmetic and Polynomial Time Hierarchy. Annals of Pure and Applied Logic, 75, .pp67-77.

Buss,S. R. (1998). Handbook of Proof Theory.Amsterdam: Elsevier.

Chang, C. C., Keisler, J. (1990).Model theory, Amsterdam: North-Holland.

Cook, S. A. (1975). Feasibly Constructive Proofs and the Propositional Calculus(preliminary version). Seventh Annual ACM Symposium on Theory of Computing,83-97.

Cook,S. A. (2009). Review of ThreePapers Relating the Collapse of the Polynomial Hierarchy to the Collapse of Bounded Arithmetic.http://www.cs.toronto.edu/~sacook/.

Cook,S. A., Urquhart,A. (1993). Functional Interpretations of Feasibly Constructive Arithmetic. Annals of Pure and Applied Logic, 63, pp. 103-200.

Hajek, P.,Pudlak, P. (1993).Metamathematics of First-order Arithmetic. Berlin: Springer-Verlag.

Hodges, H. (1997). A Shorter Model Theory. Cambridge: Cambridge University Press.

Kaye, R. (1991).Models of Peano Arithmetic. Oxford: Oxford University Press.

Krajicek, J. (1995). Bounded Arithmetic, Propositional Logic,and Complexity Theory. Cambridge: Cambridge University Press.

Krajicek, J. ,Pudlak, P., Takeuti, G. (1991).Bounded Arithmetic and the Polynomial Hierarchy. Annals of Pure and Applied Logic, 52, pp. 143-153.

Marker, D. (2002). Model Theory: An Introduction. New York: Springer-Verlag.

Moniri, M. (2006). An independence result for intuitionistic bounded arithmetic. Journal of Logic and Computation, 16, pp. 199-204.

Moniri, M. (2007). Preservation Theorems for Bounded Formulas. Archive for Mathematical Logic, 46, pp. 9-14.

Parikh, R. J. (1971). Existence and feasibility in arithmetic, Journal of Symbolic Logic, 36, pp. 494–508.

Parikh, R. J. (1973). Some results on the lengths of proofs, Transactions of the American Mathematical Society, 177, pp. 29–36.

Zambella, D. (1996). Notes on Polynomially Bounded Arithmetic, Journal of Symbolic Logic, 61, pp. 942-966.