DOR: https://csj.isi.org.ir/article_256408.html

DOI: https://doi.org/10.22034/csj.2026.555613.1133

پاییز ۱۴۰۵، دوره ۱۱، شماره ۳، پیاپی ۴۲

دریافت مقاله: ۱۴۰۴/۰۵/۳۱

پذیرش مقاله: ۱۴۰۴/۱۰/۰۶

نوع مقاله: مروری

معرفی نظام برهان‌های وارسی‌پذیر احتمالی در نظریهٔ پیچیدگی رایانشی و ابهام استفاده از اصطلاح اوراکل در این نظام

عرفان محرم زاده

دانشجوی کارشناسی ارشد علوم رایانه-محاسبات علمی، دانشکده ریاضی، دانشگاه تحصیلات تکمیلی علوم پایه زنجان، زنجان، ایران

پست الکترونیکی: erfan.mz@iasbs.ac.ir

محسن هوشمند*

استادیار، دانشکده علوم رایانه و فناوری اطلاعات، دانشگاه تحصیلات تکمیلی علوم پایه زنجان، زنجان، ایران

پست الکترونیکی: mohsenhoshmand@gmail.com

چکیده

قضیهٔ برهان‌های وارسی‌پذیر احتمالی، که به اختصار آن را پی‌سی‌پی می‌نامیم، به‌منظور اثبات نتایج مربوط به عدم تقریب‌پذیری معرفی شده است. نظام مزبور تعریفی نو از رده‌های پیچیدگی، اعم از P و NP، ارائه نموده و ابزاری قدرتمند جهت واکاوی پرسش‌های بنیادین و حل‌نشده نظریهٔ پیچیدگی محاسباتی فراهم آورده است. مقاله حاضر ابتدا ساختار نظام پی‌سی‌پی را بررسی و معرفی می‌کند و سپس، عدم تقریب‌پذیری الگوریتم‌ها را به‌عنوان یکی از نتایج اصلی قضیهٔ پی‌سی‌پی تبیین می‌نماید. در این میان، «اوراکل» یکی از اصطلاحات کلیدی در حوزهٔ تحقیقاتی پی‌سی‌پی است که در استدلال‌های عدم تقریب‌پذیری کاربرد دارد. اگرچه اوراکل در نظریهٔ محاسبات کلاسیک به‌مثابهٔ جعبه‌سیاهی با توانایی حل مسائل رایانش‌ناپذیر تلقی می‌شود، اما در چارچوب پی‌سی‌پی، این واژه صرفا بیانگر دسترسی تصادفی و آنی به بیت‌های رشتهٔ برهان است. قضیهٔ پی‌سی‌پی بر پایه همین دسترسی کارآمد و مبتنی بر احتمالات استوار است. پژوهش حاضر نشان می‌دهد کاربرد مفهوم اوراکل در حوزهٔ پی‌سی‌پی، تمایزی ماهیتی با ماشین‌های تورینگ مجهز به اوراکل دارد. به‌طور خلاصه، اوراکل در پی‌سی‌پی نه عملیات محاسبه‌ناپذیر، بلکه مدلی انتزاعی از دسترسی به حافظه است؛ حال آن که در مدل‌های فرارایانشی، دلالت بر توانایی‌های فراتر از ماشین تورینگ دارد. بنابراین، خلط این دو مفهوم می‌تواند اعتبار اثبات‌های عدم تقریب‌پذیری را به اشتباه مخدوش سازد.

کلیدواژه ها: نظریه پیچیدگی، نظام برهان‌های وارسی‌پذیر احتمالی، PCP، NP=P، اوراکل، تقریب‌ناپذیری مسائل سخت.

۱- مقدمه

ارزیابی دشواری حل مسائل و تبیین روابط میان آنها، هسته‌ی اصلی نظریهٔ پیچیدگی محاسباتی را تشکیل می‌دهد. پیچیدگی هر مسئله بر اساس منابع مجانبی مورد نیاز جهت حل آن، نظیر زمان اجرا و حافظه، تعریف و سنجیده می‌شود. از جمله قضایای بنیادین در این حوزه،

* نویسندهٔ مسئول

قضیهٔ کوک-لوین[1] است [۱] که رهیافتی برای اثبات هم‌ارزی سختی مسائل ارائه می‌دهد. تبیین رابطهٔ میان ردهٔ پیچیدگی NP (ردهٔ مسائلی که راه‌حل آنها به آسانی سنجیده نمی‌شود) و ردهٔ P (ردهٔ مسائلی که راه‌حل آنها به‌آسانی یافت می‌شود)، از مباحث چالش‌برانگیز این حوزه به‌شمار می‌رود. به بیان دقیق‌تر، مسائل ردهٔ P مسائلی هستند که یافتن راه‌حل آنها در ماشین تورینگ معین در زمان چندجمله‌ای قابل دستیابی است، و ردهٔ NP مسائلی هستند که یافتن راه‌حل آنها در ماشین تورینگ نامعین در زمان چندجمله‌ای قابل [۱].

هدف اصلی و پرسش محوری این پژوهش، بررسی دقیق جایگاه مفهوم «اوراکل» در اثبات‌های مبتنی بر پی‌سی‌پی و رفع ابهاماتی است که ممکن است از اشتراک لفظی با اوراکل‌های کلاسیک ناشی شود. در نظریهٔ پیچیدگی محاسباتی، اوراکل مفهومی انتزاعی است که به‌عنوان «جعبه‌سیاه» مدل‌سازی می‌شود و قادر است مجموعه‌ای از مسائل تصمیم را در یک گام محاسباتی بدون صرف هزینهٔ زمانی یا فضایی پاسخ دهد.

مسئلهٔ نابرابری یا برابری P و NP چندین دهه است که ذهن پژوهشگران علوم رایانه نظری را به خود معطوف داشته و به‌عنوان یکی از مهمترین پرسش‌های باز ریاضیات شناخته می‌شود[۲].

جهت پاسخگویی به این مسئله، بُن‌انگاره‌های گوناگونی پیشنهاد شده است. یکی از نخستین رویکردها، استفاده از «نسبی‌سازی[2]» بود که بیکر، گیل و سولووی در سال ۱۳۵٤ نشان دادند این روش برای اثبات یا رد برابری P و NP ناکارآمد است[۲]. از دیگر بُن‌انگاره‌های مطرح در این زمینه، می‌توان به پیچیدگی مداری[3] اشاره نمود [۱].

در اواخر دهه شصت شمسی، مفهوم نوینی تحت عنوان «برهان‌های وارسی‌پذیر احتمالی» (پی‌سی‌پی) به‌عنوان رویکردی جدیدی جهت بررسی مسئلهٔ P در برابر NP در نظریهٔ پیچیدگی محاسباتی معرفی گردید [۱]. بنیان نظری پی‌سی‌پی بر این اصل استوار است که با بهره‌گیری از بیت‌های تصادفی و وارسی بخش بسیار کوچکی از برهان طولانی، می‌توان با ضریب اطمینان بالایی نسبت به صحت راه‌حل اطمینان حاصل کرد. این مفهوم منجر به تدوین «قضیهٔ پی‌سی‌پی» شده است که علاوه بر بازتعریف رده‌های پیچیدگی، در اثبات عدم وجود الگوریتم‌های تقریبی کارآمد برای مسائل NP نیز کاربرد اساسی دارد [۱].

تمایز محاسبات احتمالاتی و تصادفی: پیش از ورود به مباحث اصلی، ضروری است تمایز میان دو مفهوم محاسبات احتمالاتی[4] و تصادفی[5] تبیین گردد. در این نوشتار، منظور از الگوریتم‌های تصادفی، الگوریتم‌هایی نظیر رده‌های BPP یا RP هستند که در طول فرایند اجرا از بیت‌های تصادفی جهت تصمیم‌گیری بهره می‌برند. در مقابل، در نظام پی‌سی‌پی، واژه احتمالاتی عمدتاً به ماهیت فرایند «وارسی» ارجاع دارد. فرایندی که در آن برهان‌سنج با مشاهده بخش محدودی از برهان و با اتکا به اصول احتمالات، حکمی کلی در باب صحت برهان صادر می‌نماید

ساختار مقاله: این نوشتار به معرفی مبانی، مقدمات و پیامدهای قضیهٔ پی‌سی‌پی می‌پردازد. ساختار مقاله به شرح ذیل سازمان‌دهی شده است. فصل ۲ به بررسی برهان‌های رایانشی کلاسیک و محدودیت‌های ذاتی آنها اختصاص دارد. در فصل ۳ ضمن تعریف پی‌سی‌پی، تمایز برهان‌های این نظام با رویکرد کلاسیک و قدرت ناشی از ماهیت احتمالاتی آن تشریح می‌گردد. فصل ٤ راهکارهای بهبود ویژگی صحت و رابطهٔ میان پیچیدگی پرس‌وجو و شکاف مورد بحث قرار می‌گیرد. در فصل ۵ قضیهٔ پی‌سی‌پی و دلالت‌های آن بر دشواری یافتن الگوریتم‌های تقریبی واکاوی می‌شود. در فصل ٦ مروری اجمالی بر مفهوم اوراکل و جایگاه آن در نظریهٔ محاسبات ارائه می‌گردد. در فصل ۷ به تحلیل ابهامات ناشی از کاربرد اصطلاح اوراکل در تعریف برهان‌سنج نظام پی‌سی‌پی پرداخته خواهد شد. شایان ذکر است، پیش‌فرض این نوشتار آشنایی خواننده با

1-Cook-Levin
2-Relativization
3-Circuit Complexity
4-Probabilistic
5-Randomized

مفاهیم مقدماتی پیچیدگی رایانشی، از جمله مسائل تصمیم، ماشین‌های تورینگ معین و نامعین، و مسئلهٔ صدق‌پذیری (از جمله صدق-۳[6]) است.

۲- برهان رایانشی کلاسیک در نظریهٔ پیچیدگی رایانشی

محققان همواره در تلاش برای تعیین کوچک‌ترین ردهٔ پیچیدگی ممکن برای هر مسئلهٔ تصمیم و اثبات تعلق آن مسئله به ردهٔ مذکور هستند. این اثبات‌ها ماهیتاً از نوع «اثبات رایانشی» محسوب می‌شوند. به‌عنوان نمونه، اثبات تعلق مسئلهٔ صدق-۳ به ردهٔ NP از دو طریق امکان‌پذیر است که هر دو بر پایهٔ اصول اثبات‌های رایانشی استوارند

در روش نخست، با بهره‌گیری از ماشین تورینگ نامعینْ تلاش می‌شود تا در شاخه‌های محاسباتی مختلف، تخصیص‌های گوناگون به متغیرهای بولی تعلق گیرد. چنانچه در یکی از شاخه‌ها تخصیصی یافت شود که منجر به صدق نمونهٔ مسئله گردد، پاسخ مثبت بازگردانده می‌شود. قابل اثبات است که تعداد مراحل مورد نیاز جهت رایانش برهان با چنین ماشینی، تابعی خطی از تعداد متغیرها (n) و تعداد بندهای مسئله (l) است. لذا پیچیدگی زمانی از مرتبهٔ چندجمله‌ای ($O(n+l)$) بوده و مسئله به ردهٔ NP تعلق دارد.

روش دوم، مبتنی بر استفاده از ماشین تورینگ معین است. در این رویکرد، برای هر نمونه از مسئلهٔ صدق-۳، یک «گواه[7]» ارائه می‌شود. اعتبارسنجی پاسخ پیشنهادی نیازمند زمانی متناسب با تعداد متغیرها (n) و تعداد جملات (l) است ($O(n+l)$). بنابراین، ماشین تورینگ معین قادر است در تعداد گام‌های مذکور، صحت راه‌حل (گواه) را بررسی نماید. این روش نیز مؤید عضویت مسئله در ردهٔ NP است. شایان ذکر است که در این رویکرد، گواهی از پیش مشخص بوده و صرفاً صحت آن در زمان چندجمله‌ای ارزیابی می‌شود.

این الگوی اثبات در رده‌ای تحت عنوان «برهان تعاملی[8]» تعمیم می‌یابد. در این ساختار، «برهان‌ساز[9]» با قدرت محاسباتی نامحدود می‌کوشد تا گواهی دال بر درستی نمونه را بیابد. سپس، این گواه به «برهان‌سنج[10]» با قدرت محاسباتی محدود ارائه می‌شود. هدف برهان‌ساز، متقاعد ساختن برهان‌سنج نسبت به صحت گواه است، حتی اگر برهان وی عمداً یا سهواً نادرست باشد. در مقابل، برهان‌سنج با بهره‌گیری از منابع محدود خود، به ارزیابی گواه می‌پردازد. چنانچه برهان‌سنج به‌صورت قطعی و معین عمل نماید، این رده معادل NP خواهد بود [۳]. اما در صورتی که برهان‌سنج از عنصر تصادف بهره جوید، ردهٔ پیچیدگی IP شکل می‌گیرد که از توان محاسباتی بسیار بالایی برخوردار بوده و با ردهٔ PSPACE برابری می‌کند [۳]. در غیاب ماهیت احتمالاتی در عملکرد برهان‌سنج، برهان‌ساز فریبکار قادر خواهد بود پاسخی طراحی کند که برهان‌سنج را گمراه سازد. به بیان دیگر، اگر برهان‌سنج معین باشد و از تصادف (مدل‌سازی شده با پرتاب سکه) استفاده نکند، برهان‌ساز می‌تواند با تحلیل تمامی حالات ممکن، پاسخی ارائه دهد که به تأیید نادرست منجر شود. بدین منظور، دو مفهوم بنیادین زیر تعریف می‌شوند [۱، ۳]

- **تمامیت**[11]: این ویژگی تضمین می‌کند اگر گزاره‌ای واقعا صحیح باشد (مثلا معادله بولی صدق‌پذیر باشد)، برهان‌ساز صادق می‌تواند برهان‌سنج را با احتمال بالا (معمولا ۱) قانع کند تا آن را بپذیرد.
- **صحت**[12]: این ویژگی تضمین می‌کند اگر گزاره‌ای نادرست باشد (مثلا معادله بولی صدق‌ناپذیر باشد)، هیچ برهان‌سازی (حتی فریبکار با قدرت نامحدود) نمی‌تواند برهان‌سنج را با احتمالی بیش از حد خطای مشخص (مثلا s) قانع کند تا آن را بپذیرد.

۳- نظام برهان‌های وارسی‌پذیر احتمالی (پی‌سی‌پی)

در ادامه، جهت تبیین سازوکار پی‌سی‌پی، مسئلهٔ صدق-

6-3-SAT
7-Witness
8-Interactive Proof
9-Prover
10-Verifier
11-Completeness
12-Soundness

۳ بررسی می‌شود. در مسئلهٔ صدق-۳، نادرست بودن تخصیص پیشنهادی بدین معناست که دست‌کم یکی از بندها صادق نشده و در نتیجه کل معادله فاقد اعتبار است. بنابراین، برای رد ادعا، کافی است برهان‌سنج تنها همان بند ناقض را شناسایی نماید. به بیان دیگر، تنها به بررسی سه بیت از برهان نیاز است. چالش اصلی در اینجا، یافتن روشی کارآمد برای دسترسی به این بیت‌های خاص (برای گزارش صدق‌پذیر نبودن معادله) است. نظام پی‌سی‌پی در این موقعیت وارد صحنه می‌شود. اگرچه پی‌سی‌پی ابتدا با اهدافی در حوزهٔ رمزنگاری و پیچیدگی محاسباتی معرفی شد [٤]، اما به‌سرعت کارآمدی خود را در برهان‌هایی مشابه مثال فوق نشان داد. برخلاف سیستم‌های برهان تعاملی متعارف که مبتنی بر تبادل پیام میان برهان‌ساز و برهان‌سنج هستند، در نظام پی‌سی‌پی، برهان‌ساز کل برهان را به‌صورت یکجا در اختیار برهان‌سنج قرار می‌دهد. در این نظام، برهان‌ها در قالبی خاص که دارای «افزونگی[۱۳]» است تدوین شده و با نماد π نمایش داده می‌شوند [٥].

مثال ۳.۱. معادله حل‌ناپذیر صدق-۳ زیر را با ۳ متغیر و ۳ بند در نظر می‌گیریم:

$$\phi = (x \vee y \vee \neg z) \wedge (\neg x \vee y \vee z) \wedge (x \vee \neg y \vee z)$$

در اثبات کلاسیک، برهان رشتهٔ $x = (111)$ است که مقادیر متغیرها را نشان می‌دهد. برهان‌سنج کلاسیک ناگزیر است تمام بندها را بررسی کند. اما در نظام پی‌سی‌پی، برهان π دارای ساختاری با افزونگی با جداکننده‌های # است که در جدول زیر تشریح شده است:

شرح بخش‌های برهانِ $\pi = 111\#110\#011\#101$		
بخش‌های برهان (π)	محتوا (بیت)	توضیحات
بخش اول	۱۱۱	مقداردهی متغیرها (x, y, z)
بخش دوم	۱۱۰	مقداردهی بند اول به ازای متغیرها
بخش سوم	۰۱۱	مقداردهی بند دوم به ازای متغیرها
بخش چهارم	۱۰۱	مقداردهی بند سوم به ازای متغیرها

13-Redundancy

برهان‌سنج پی‌سی‌پی قابلیت دسترسی آنی به تمامی بیت‌های برهان را داراست [۱]. تعاریف رسمی برهان و برهان‌سنج در این نظام به شرح زیر است:

تعریف ۳. ۱. (برهان در نظام پی‌سی‌پی): رشته‌ای دودویی به طول k بیت است که با نماد π نشان داده می‌شود. از آنجا که برهان‌سنج دسترسی آنی به هر بیت دارد، برهان به‌عنوان تابع $\pi: \{1, \dots, k\} \to \{0,1\}$ مدل‌سازی می‌شود.

تعریف ۳. ۲. (برهان‌سنج در نظام پی‌سی‌پی): الگوریتمی احتمالی است که با دریافت رشتهٔ $A \in \{0,1\}^n$ و انتخاب رشتهٔ تصادفی $R \in \{0,1\}^*$، پرس‌وجوهای آنی[۱٤] را بر روی برهان انجام داده و بر اساس آن، به‌صورت احتمالاتی حکم به پذیرش یا رد می‌دهد.

در نظام پی‌سی‌پی دو نوع برهان‌سنج «تطبیقی[۱٥]» و «غیرتطبیقی[۱٦]» قابل تصور است. در نوع تطبیقی، انتخاب بیت‌های بعدی جهت پرس‌وجو وابسته به پاسخ‌های دریافتی پیشین است. حال آن که در نوع غیرتطبیقی، تمامی مکان‌های موردنظر برای پرس‌وجو در ابتدای امر، صرفا بر اساس ورودی تصادفی تعیین می‌گردند [٥].

۳-۱- اهمیت ماهیت احتمالاتی

برهان‌سنجی پی‌سی‌پی صرفا با خواندن تعداد محدودی از بیت‌های برهان در خصوص صحت آن تصمیم‌گیری می‌کند. چنانچه عملکرد برهان‌سنج قطعی[۱۷] باشد، برهان‌ساز فریبکار می‌تواند با تحلیل پیشاپیش رفتار برهان‌سنج، برهانی ساختگی ایجاد کند تا دقیقا در نقاط مورد بررسی، صحیح باشند. از آنجا که پیچیدگی زمانی این جست‌وجو $O(2^k)$ است و برهان‌ساز دارای توان نامحدود فرض می‌شود، این امر امکان‌پذیر است. بنابراین، عنصر تصادف در انتخاب پرس‌وجوها نقشی حیاتی ایفا می‌کند. به بیان دیگر، فرایندهای قطعی مزیتی فراتر از نظام اثبات رایانشی NP ایجاد نمی‌کنند. تصادفی بودن برهان‌سنج موجب پیش‌بینی‌ناپذیری آن شده و در نتیجه، امکان فریب سیستم را از برهان‌ساز سلب می‌کند.

14-Random Access
15-Adaptive
16-Non-adaptive
17-Deterministic

۲-۳- تعاریف بنیادین

در این بخش، مفاهیم کلیدی پی‌سی‌پی نظیر پیچیدگی پرس‌وجو، پیچیدگی تصادفی و شکاف بر اساس مرجع [٤] تعریف می‌شوند.

تعریف ۳-۳. (**پیچیدگی پرس‌وجو**[18]): تابع $q:\mathbb{N}\to\mathbb{N}$ است. برای ورودی به طول n بیت، برهان‌سنج حداکثر $q(n)$ «پرس‌وجوی آنی» انجام می‌دهد. این پارامتر بیانگر تعداد بیت‌هایی از برهان است که جهت اعتبارسنجی خوانده می‌شوند.

تعریف ۳-۴. (**پیچیدگی تصادفی**[19]): تابع $r:\mathbb{N}\to\mathbb{N}$ است که حداکثر تعداد بیت‌های تصادفی (سکه) موردنیاز برهان‌سنج برای ورودی به طول n بیت را تعیین می‌کند. این رشتهٔ تصادفی (ω) مسیر اجرا و نقاط هدف پرس‌وجو را مشخص می‌سازد.

تعریف ۳-۵. (**شکاف**[20]): این مفهوم کمّیتی برای سنجش توانایی تفکیک برهان‌سنج میان گزاره‌های صحیح و ناصحیح است و به صورت $\varepsilon(n)=c-s$ تعریف می‌شود. در این تعریف، c احتمال پذیرش گزارهٔ درست (که در اینجا ۱ فرض می‌شود) و s حداکثر احتمال پذیرش گزارهٔ نادرست است. بنابراین $\varepsilon(n)=1-s$، هر چه مقدار شکاف بزرگ‌تر باشد، احتمال خطای s کمتر است.

تعریف ۳-۶. (**مکان مرتبط**[21]): به مکان بیت i–ام در رشتهٔ برهان که طی فرایند بررسی مورد پرس‌وجو قرار می‌گیرد، مکان مرتبط اطلاق می‌شود.

تعریف ۳-۷. (**طول مؤثر برهان**[22]): کوچکترین کران بالا برای تعداد بیت‌های مرتبط برهان به ازای ورودی x است. این پارامتر حداقل اطلاعات واقعا موردنیاز از برهان را می‌سنجد و دارای کران بالای 2^{r+q} است.

۳-۳- ردهٔ پیچیدگی پی‌سی‌پی

تعریف ۳-۸. (**ردهٔ پیچیدگی $PCP(r,q)$**): مجموعه زبان‌هایی است که برای آنها برهان‌سنج پی‌سی‌پی با پیچیدگی تصادفی $r(n)$ و پیچیدگی پرس‌وجوی $q(n)$ وجود دارد [٦]. ردهٔ جامع $PCP(R,Q)$ اجتماع تمام رده‌های $PCP(r,q)$ است که در آن $r\in R$ و $q\in Q$ باشند [٥].

قضایای زیر ارتباط میان رده‌های پی‌سی‌پی و رده‌های کلاسیک را تبیین می‌کنند:

قضیه ۳-۱. $\boldsymbol{PCP(0,0)=P}$. استدلال: عدم وجود تصادف و پرس‌وجو معادل تصمیم‌گیری قطعی بدون بررسی برهان است که با ردهٔ P هم‌ارز است.

قضیه ۳-۲. $\boldsymbol{PCP(O(\log n),0)=P}$. استدلال: با وجود بیت‌های تصادفی لگاریتمی اما بدون مراجعه به برهان، ماشین تورینگ قادر است تمام حالات تصادفی را در زمان چندجمله‌ای شبیه‌سازی کند.

قضیه ۳-۳. $\boldsymbol{PCP(O(1),O(\log n))=P}$. استدلال: با تصادف ثابت، برهان همچون رشته‌ای با طول لگاریتمی خواهد بود که بررسی آن در زمان چندجمله‌ای مقدور است.

قضیه ۳-۴. $\boldsymbol{PCP(0,poly(n))=NP}$. استدلال: برهان سنجی قطعی که مجاز به خواندن تعداد چندجمله‌ای بیت از برهان باشد، دقیقا منطبق بر تعریف کلاسیک NP است.

قضیه ۳-۵. فرض کنیم $S\epsilon PCP(r,q)$ است. زبان S می‌تواند توسط ماشین تورینگ نامعینی تصمیم‌گیری شود که حداکثر $2^{r(n)}.q(n)$ گام غیرقطعی داشته و در مجموع در $2^{r(n)}.poly(n)$ گام متوقف گردد. اثبات: هدف، طراحی ماشین تورینگ نامعینی است که دقیقا زبانی را بپذیرد که توسط برهان‌سنج $PCP(r,q)$ پذیرفته می‌شود. این ماشین با دریافت ورودی x، رویکرد زیر را اتخاذ می‌کند: ۱. از آنجا که ماشین به رشتهٔ تصادفی ω دسترسی مستقیم ندارد، تمامی $2^{r(n)}$ حالت ممکن برای رشته‌های تصادفی را مدنظر قرار می‌دهد. ۲. ماشین به‌ازای هر رشتهٔ تصادفی، $q(n)$ بیت موردنیاز از برهان را به‌صورت غیرقطعی حدس می‌زند و سپس بررسی می‌کند که آیا این حدس‌ها منجر به پذیرش توسط برهان‌سنج می‌شوند یا خیر. از آنجا که عملیات بررسی برای هر رشتهٔ تصادفی در زمان چندجمله‌ای $(poly(n))$ انجام می‌پذیرد، پیچیدگی زمانی نهایی حاصل‌ضرب تعداد حالات تصادفی در زمان بررسی

18-Query Complexity
19-Randomness Complexity
20-Gap
21-Relevant Location
22-Effective Proof Length

هر حالت، یعنی $poly(n).2^{r(n)}$ خواهد بود.

لم ۳- ۱. هر زبان تصمیم‌گیری شده در ماشین تورینگ نامعین در زمان $T(n)$، در ماشین تورینگ معین در زمان $2^{O(T(n))}$ قابل تصمیم‌گیری است.

قضیه ۳-۶. $\boldsymbol{PCP(r,q) \subseteq DTIME(2^{2^{r(n)}.q(n)}.r(n).poly(n))}$

اثبات: بنابر قضیهٔ ۵،۳، هر زبان $L \in PCP(r,q)$ را می‌توان به کمک ماشین تورینگ نامعین شبیه‌سازی کرد. این ماشین برای بررسی ورودی، نیاز دارد مقادیر بیت‌های برهان را بداند. از آنجا که برهان‌سنج به ازای هر یک از $2^{r(n)}$ رشتهٔ تصادفی ممکن، حداکثر $q(n)$ بیت را می‌خواند، تعداد کل بیت‌های برهان که در فرایند تصمیم‌گیری مؤثرند، حداکثر $M = 2^{r(n)}.q(n)$ بیت است. ماشین نامعین می‌تواند این M بیت را به‌صورت غیرقطعی حدس بزند. بنابراین، با استناد به لم ۱،۳، ماشین تورینگ معین می‌تواند با پیمایش تمامی 2^M حالت ممکن برای این بیت‌ها، وجود برهان معتبر را بررسی کند. زمان لازم برای این شبیه‌سازی معین، متناسب با تعداد حالات $2^{2^{r(n)}.q(n)}$ ضرب در زمان اعتبارسنجی هر حالت (که تابعی از $r(n)$ و $poly(n)$ است) خواهد بود. بدین‌ترتیب، شمول در ردهٔ زمانی $DTIME$ مذکور اثبات می‌گردد.

قضیه ۳-۷. $\boldsymbol{PCP(0, O(1)) = P}$. اثبات: با جایگذاری مقادیر $r = 0$ و $q = O(1)$ در قضیهٔ ۳.٦، نتیجهٔ $DTIME(poly(n))$ حاصل می‌شود که همان P است.

۴- تحلیل رابطهٔ پیچیدگی پرس‌وجو و شکاف

۴-۱- مقایسهٔ برهان‌سنج کلاسیک و پی‌سی‌پی

در مدل کلاسیک، برهان‌سنج تمام برهان را مطالعه می‌کند. لذا می‌توان آن را برهان‌سنج پی‌سی‌پی با پیچیدگی پرس‌وجوی بالا ($q(n) = n$) و شکاف کامل ($\varepsilon(n) = 1$) دانست. در مقابل، نسخهٔ احتمالاتی ساده‌ای را در نظر بگیریم که تنها یک بند تصادفی را بررسی می‌کند. در اینجا q ثابت و بسیار کوچک است، اما شکاف $\varepsilon(n) = 1/m$ خواهد بود که با افزایش ابعاد مسئله به صفر میل می‌کند [٤]. پرسش اساسی این است که آیا می‌توان همزمان به شکاف بزرگ و پیچیدگی پرس‌وجوی پایین دست یافت؟ قضیهٔ پی‌سی‌پی پاسخی مثبت به این پرسش می‌دهد.

۴-۲- بهبود ویژگی صحت از طریق تکرار

برای بهبود ویژگی صحت، فرایند وارسی t بار تکرار می‌شود. با این کار، احتمال خطای برهان‌سنج به‌صورت نمایی (s^t) کاهش می‌یابد، در حالی که هزینهٔ پیچیدگی پرس‌وجو و تصادف به‌صورت خطی (ضریب t) افزایش می‌یابد. احتمال فریب خوردن برهان‌سنج به میزان s^t کاهش می‌یابد. پیچیدگی‌های پرس‌وجو و تصادفی نیز به اندازه‌ی ضریب t افزایش می‌یابند.

مثال ۴-۱. (تکرار متوالی جهت کاهش خطا): فرض کنیم سیستم پی‌سی‌پی‌ای دارای خطای صحت[23] برابر با $s = 1/2$ است. به این معنی که در هر بار اجرا، شانس این که برهان‌ساز فریبکار بتواند برهان‌سنج را نسبت به گزاره‌ای نادرست متقاعد کند، ۵۰ درصد است. حال اگر هدف دستیابی به سطح اطمینان ۹۹/۹ درصد باشد (یعنی احتمال خطا به کمتر از ۰،۰۰۱ برسد)، برهان‌سنج باید آزمون را تکرار کند. با انجام t بار تکرار مستقل، احتمال خطای کل به s^t کاهش می‌یابد. در این حالت، برای برقراری شرط $(1/2)^t < 0.001$، با توجه به این که $2^{10} = 1024$، انتخاب $t = 10$ خطای $(1/2)^{10} \approx 0.00097$ را نتیجه می‌دهد که کمتر از حد آستانهٔ مجاز است. بنابراین، با ده بار تکرار ضریب اطمینان به حد مطلوب ارتقا می‌یابد.

۵- قضیهٔ پی‌سی‌پی و پیامدهای آن

یکی از دستاوردهای برجستهٔ نظریهٔ پیچیدگی، قضیهٔ پی‌سی‌پی است که آرورا[24] و همکاران (۱۹۹۸) اثبات کردند [٦]

قضیه ۵-۱. (قضیهٔ پی‌سی‌پی):

$$\boldsymbol{PCP(O(\log n), O(1)) = NP}$$

این قضیه بیان می‌دارد که هر مسئلهٔ متعلق به ردهٔ NP را می‌توان با استفاده از تعداد لگاریتمی بیت تصادفی

23-Soundness Error
24-Arora

و پرس‌وجوی تعداد ثابتی از بیت‌های برهان، با دقت بالا وارسی نمود.

مثال ۵-۱. جهت تبیین دقیق‌تر، معادله صدق-۳ حل‌ناپذیر فرضی را در نظر بگیریم. فرض کنیم برهان‌ساز فریبکار، برهانی ساختگی (π) ارائه کرده است. در این برهان، برای یکی از بندها مقداردهی نادرستی درج شده است (برای نمونه، فرض کنیم مقداردهی صحیح باید ۰۰۰ باشد که نشان‌دهندهٔ عدم صادق شدن بند است، اما برهان‌ساز مقدار دیگری درج کرده است). برهان‌سنج موظف است در فرایند پرس‌وجوی تصادفی خود، دو شرط را احراز نماید: نخست آن که در مقداردهی ارائه شده برای هر بند، دست‌کم ارزش یک بیت برابر با ۱ باشد (شرط صدق‌پذیری). دوم آن که بیت‌های منتسب به بند، با مقادیر متغیرهای متناظر در بخش اول برهان و ساختار خود بند سازگاری داشته باشند (شرط تطابق). برهان‌سنج به‌صورت تصادفی بخش دوم برهان را انتخاب می‌کند (که به فرض مقدار ۰۱۱ را دارد). بررسی شرط اول نشان می‌دهد این بخش دارای بیت با مقدار ۱ است (شرط صدق‌پذیری برقرار است). در بررسی شرط دوم، با توجه به مقداردهی متغیرها در بخش اول برهان (مثلا ۱۱۱) و ساختار بند دوم (که لیترال‌های آن به گونه‌ای است که با مقادیر متغیرها سازگار است)، تطابق مقادیر تأیید می‌شود. بدین‌ترتیب، برهان‌ساز توانسته است در این بررسی موضعی، برهان‌سنج را فریب دهد.

این مثال، درک سازوکار قضیهٔ ۵-۱ را تسهیل می‌کند. اگر فرمول دارای n بند باشد، می‌توان هر بند را با یک عدد در بازهٔ ۱ تا n آدرس‌دهی نمود. برهان‌سنج با انتخاب تصادفی یک عدد در این بازه، نیازمند $O(\log n)$ بیت تصادفی است. از سوی دیگر، در هر نوبت وارسی، تنها نیاز به خواندن تعداد محدودی بیت از برهان دارد (مثلا ۳ بیت مربوط به بند و ۳ بیت مربوط به متغیرها)، که بیانگر پیچیدگی پرس‌وجوی ثابت $O(1)$ است.

۵-۱. عدم وجود الگوریتم‌های تقریبی کارآمد

قضیهٔ پی‌سی‌پی ارتباط تنگاتنگی با دشواری تقریب مسائل NP-hard دارد. اگر فرض کنیم $P \neq NP$، قضیهٔ پی‌سی‌پی نشان می‌دهد که یافتن الگوریتم‌های تقریبی با دقت بالا برای بسیاری از مسائل NP دشوار است. کلید این ارتباط، در مفهومی به نام «کاهش پی‌سی‌پی[۲۵]» نهفته است

مفهوم کاهش پی‌سی‌پی [۱، ۶]: تبدیل چندجمله‌ای است که برخلاف کاهش‌های کلاسیک، «شکاف» میان مقادیر بهینهٔ مسئله در حالات «بله» و «خیر» را ایجاد می‌کند. در این کاهش:

- تمامیت: اگر پاسخ مسئلهٔ اصلی «بله» باشد، مقدار بهینه‌ی مسئلهٔ حاصل حداکثر ممکن (مثلا ۱۰۰٪) است.
- صحت: اگر پاسخ مسئلهٔ اصلی «خیر» باشد، مقدار بهینه‌ی مسئلهٔ حاصل از حد آستانه‌ای مشخص (مثلا s) کمتر است. این شکاف ایجاد شده تضمین می‌کند که هر الگوریتم تقریبی که بتواند جوابی بهتر از آستانهٔ s بیابد، در واقع قادر است مسئلهٔ اصلی NP-hard را حل کند.

تعریف ۵-۱. (**مسئلهٔ** MAX-3SAT): هدف این مسئله، یافتن تخصیصی است که بیشترین تعداد بندهای فرمول بولی را صادق نماید.

استدلال بر عدم تقریب‌پذیری: فرض کنیم الگوریتمی تقریبی موسوم به «الف» وجود دارد که قادر است همواره پاسخی با دقت ۸۰ درصد برای MAX-3SAT بیابد. با بهره‌گیری از این الگوریتم و ساختار کاهش پی‌سی‌پی (که در آن خطای صحت s کمتر از ۸۰ درصد تنظیم شده است)، می‌توان الگوریتم تصمیم‌گیر جدیدی (که آن را «الف ستاره» می‌نامیم) طراحی نمود که قادر است مسئلهٔ اصلی صدق‌پذیری را در زمان چندجمله‌ای حل کند: ۱. تبدیل: فرمول ورودی ϕ با استفاده از کاهش پی‌سی‌پی به فرمول جدید ψ تبدیل می‌شود. طبق ویژگی «تمامیت»، اگر ϕ صدق‌پذیر باشد، ψ کاملا صدق‌پذیر است (۱۰۰ درصد بندها). ۲. تصمیم‌گیری: اگر ϕ صدق‌پذیر باشد، الگوریتم

25-PCP Reduction

«الف» عددی بالای ۸۰ درصد را بازمی‌گرداند. اما اگر ϕ صدق‌ناپذیر باشد، طبق ویژگی «صحت» و وجود «شکاف» ایجاد شده توسط پی‌سی‌پی، امکان تمایز قطعی میان حالات صدق‌پذیر و صدق‌ناپذیر را با الگوریتمی تقریبی فراهم می‌سازد. لذا وجود چنین الگوریتم تقریبی مستلزم $P = NP$ خواهد بود.

نتیجه ۵-۱. مسئلهٔ MAX-3SAT در ردهٔ مسائل NP-hard است [۱].

نتیجه ۵-۲. اگر الگوریتم تقریبی دقیق برای بسیاری از مسائل NP موجود باشد، منجر به هم‌ارزی رده‌های P و NP خواهد شد [۱، ٦].

۶- مفهوم اوراکل در نظریهٔ پیچیدگی رایانشی

در روند طبقه‌بندی مسائل بر اساس منابع مورد نیاز، مفهوم «ماشین اوراکل» به‌عنوان ابزاری انتزاعی معرفی شده است. ماشین اوراکل، جعبه‌سیاهی فرضی است که قادر است مسائل تصمیم خاصی را بدون هزینهٔ محاسباتی و به‌صورت آنی حل نماید [۷]. زبانی که اوراکل می‌پذیرد با A و ماشین تورینگ مجهز به آن را با M^A نمایش می‌دهند [۸]. این مفهوم در بحث «نسبی‌سازی[۲۶]» و تعریف رده‌های P^A و NP^A کاربرد اساسی دارد.

۷- واکاوی ابهام اصطلاح اوراکل در نظام پی‌سی‌پی

اصطلاح «اوراکل» در حوزهٔ تحقیقاتی پی‌سی‌پی کاربردی متفاوت از معنای کلاسیک آن دارد. در فصل ۳ اشاره شد که برهان‌سنج دسترسی آنی به بیت‌های برهان دارد. در برخی متون، به این سازوکار دسترسی نیز «اوراکل» اطلاق می‌گردد [٤، ٥]. این اشتراک لفظی میان اوراکل محاسباتی (فصل ٦) و دسترسی آنی در پی‌سی‌پی ممکن است منجر به ابهام و ایراد بر نتایج عدم‌تقریب‌پذیری الگوریتم‌ها شود.

مفهوم اوراکل، شالودهٔ بسیاری از اثبات‌های نظری است. اما اگر معنای اوراکل در نظام پی‌سی‌پی دقیقا همانند تعریف آن در فصل ٦ تفسیر شود، ابهامی جدی رخ می‌نماید. یادآوری می‌شود که در انتهای بخش پیشین، الگوریتم فرضی «الف ستاره» با اتکا به برهان‌سنج پی‌سی‌پی، فرمول جدیدی ایجاد نمود که منجر به تناقض و در نهایت اثبات عدم تقریب‌پذیری گردید. حال اگر فرض شود که برهان‌سنج پی‌سی‌پی از قدرت اوراکلی به معنای کلاسیک آن بهره می‌برد، ممکن است کل فرایند استدلال زیر سؤال برود.

لازم است پیش‌زمینه‌ای در خصوص «ماشین‌تورینگ وزن‌دار[۲۷]» [۹] و ادعای «ماشین‌های فرارایانشی[۲۸]» ارائه گردد. پس از معرفی ماشین‌تورینگ وزن‌دار، پیری ویدرمان[۲۹] [۹] ادعای قابل‌توجهی را مطرح نمود مبنی بر این که ماشین‌های تورینگ فرارایانشی می‌توانند قدرتی فراتر از ماشین‌های تورینگ استاندارد داشته باشند. با این حال، بنجامین بدرگال[۳۰] و سانتیاگو فیگوئرا[۳۱] [۱۰] این ایده را مورد نقد جدی قرار دادند. آنها استدلال کردند که تحقق ماشین فرایارانشی منوط به فرض بسیار خاصِ «توانایی ماشین برای کار با اعداد حقیقی غیرقابل رایانش» است. اعطای چنین مجوزی به منزلهٔ تجهیز ماشین به نوعی اوراکل قدرتمند است [۱۱، ۱۲]. از آنجا که وجود فیزیکی چنین اوراکلی محال است، تحقق ماشین فرارایانشی نیز منتفی است.

حال ممکن است این ابهام برای اثبات عدم تقریب‌پذیری هم رخ دهد. همان‌طور که اشاره شد، اثبات مذکور بر پایهٔ برهان‌سنج پی‌سی‌پی انجام می‌گیرد. برهان‌سنج پی‌سی‌پی نیز دارای اوراکل است و وجود این اوراکل موجب تقویت ابهام درستی در اثبات عدم تقریب‌پذیری می‌شود. اما این نتیجه‌گیری صحیح نیست. به بیان دیگر، باید به ماهیت متفاوت اوراکل‌ها در این دو حوزه توجه کرد. جدول زیر تفاوت‌های بنیادین این دو مفهم را تبیین می‌کند:

26-Relativization

27-Weighted Turing Machines
28-Hypercomputation
29-Jiří Wiedermann
30-Benjamin Bedregal
31-Santiago Figueira

تفاوت میان اوراکل ماشین تورینگ (کلاسیک) و اوراکل در نظام پی‌سی‌پی		
ویژگی	اوراکل ماشین تورینگ (کلاسیک)	اوراکل در نظام پی‌سی‌پی
ماهیت	جعبه‌سیاه محاسباتی	رشته‌ای از داده‌ها (برهان)
قدرت	حل مسائل محاسبه‌ناپذیر یا دشوار	صرفا دسترسی تصادفی به حافظه
نقش	ارتقای توان محاسباتی ماشین	مدل‌سازی دسترسی کارآمد به داده‌ها
قابلیت تحقق	انتزاعی و غیرقابل پیاده‌سازی فیزیکی	قابل شبیه‌سازی با مدل دسترسی مستقیم به حافظه

بنابراین، اوراکل در نظام پی‌سی‌پی فرضی محاسبه ناپذیر محسوب نمی‌شود و شایسته است برای اجتناب از خلط مبحث، به جای به‌کار بردن واژهٔ «اوراکل» از تعبیر دقیق‌تر «دسترسی آنی» استفاده گردد. همان‌طور که در این نوشتار رعایت شده است. در نتیجه، استدلال‌های عدم تقریب‌پذیری مبتنی بر پی‌سی‌پی کاملا معتبر بوده و نمی‌توان آن را متهم به استفاده از ابزارهای محاسبه‌ناپذیر (به مانند تعریف کلاسیک اوراکل) کرد.

۸- نتیجه‌گیری و افق‌های پژوهشی

در این نوشتار، نظام برهان‌های وارسی‌پذیر احتمالی (پی‌سی‌پی) به‌عنوان چارچوبی نو و تحول‌آفرین در نظریهٔ پیچیدگی مورد بررسی قرار گرفت. تحلیل‌ها نشان داد این نظام با ادغام معیارهای احتمالاتی و دسترسی تصادفی به برهان، ابزاری قدرتمند جهت اثبات سختی تقریب مسائل NP فراهم آورده است. نکتهٔ کلیدی پژوهش، ابهام‌زدایی از مفهوم «اوراکل» در این حوزه بود. تبیین گردید که اوراکل در پی‌سی‌پی دلالت بر دسترسی کارآمد به داده‌ها داشته و متمایز از مفهوم اوراکل در ماشین‌های تورینگ (که دلالت بر قدرت فرامحاسباتی دارد) است.

پیشنهادهایی برای پژوهش‌های آینده: بر مبنای مباحث مطرح شده، محورهای پژوهشی زیر پیشنهاد می‌گردند:

۱. بهینه‌سازی پارامترهای پی‌سی‌پی: تمرکز بر کاهش هم‌زمان پیچیدگی پرس‌وجو (q) و پیچیدگی تصادفی (r) با حفظ شکاف خطا، که نقشی حیاتی در کارایی پروتکل‌های اثبات ایفا می‌کند.

۲. کاربردهای نو در رمزنگاری: بررسی پتانسیل پی‌سی‌پی‌های کوتاه (مانند PCPs of Proximity) در توسعهٔ سیستم‌های اثبات دانش‌صفر[۳۲] مقیاس‌پذیر برای فناوری‌های توزیع‌شده و محاسبات امن.

۳. تحلیل برهان‌سنج‌های تطبیقی: مطالعهٔ عمیق‌تر تأثیر تطبیقی بودن پرس‌وجوها بر درجهٔ سختی تقریب در مسائل خاص گراف و هندسهٔ محاسباتی.

مراجع

1. Arora, S., & Barak, B. 2009. Computational complexity: a modern approach, Cambridge University Press.
2. Aaronson, S. 2016. "$P \stackrel{?}{=} NP$", Open Problems in Mathematics, pp. 1-122, Springer.
3. Sipser, M. 2012. Introduction to the theory of computation, Wadsworth Publishing.
4. Sudan, M. 2009. "Probabilistically checkable proofs", Communications of the ACM, Vol. 52, No. 3, pp. 76-84.
5. Goldreich, O. 2008. "Computational complexity: a conceptual perspective", ACM Sigact News, Vol. 39, No. 3, pp. 35-39.
6. Arora, S., & Safra, S. 1998. "Probabilistic checking of proofs: A new characterization of NP", Journal of the ACM (JACM), Vol. 45, No. 1, pp. 70-122.
7. Oreggia, E. M. I. 2013. Towards the Oracle Machine (MPhil Thesis). Goldsmiths College, University of London.
8. Alper, J. D. 2001. Oracle theory. Oracle Theory Course Notes, Brown University.
9. Wiedermann, J. 2004. "Characterizing the super-Turing computing power and efficiency of classical fuzzy Turing machines", Theoretical Computer Science, Vol. 317, No. 1-3, pp. 61-69.
10. Bedregal, B. R. C., & Figueira, S. 2006. "Classical computability and fuzzy Turing machines", Latin American Symposium on Theoretical Informatics, pp. 154-165, Springer.
11. Ord, T., & Kieu, T. D. 2005. "The diagonal method and hypercomputation", The British journal for the philosophy of science, Vol. 56, No. 1, pp. 147-156.
12. Davis, M. 2004. "The Myth of Hypercomputation", Alan Turing: Life and Legacy of a Great Thinker, pp. 195-211, Springer.

32-Zero-Knowledge Proofs