دانشکده علوم ریاضی
دانشگاه صنعتی شریف

پیچیدگی محاسبه

محمدهادی فروغمنداعرابی
بهار ۱۳۹۴

اثبات های طبیعی

۱۰ خرداد

نگارنده: عرفان خانیکی

۱ مقدمه

در جلسات قبل با استفاده از ماشین تورینگ های اوراکل دار دیدیم که با استفاده از تکنیک قطری سازی در شرایط خاصی قادر به اثبات $P = NP$ یا $P \subsetneq NP$ نیستیم. در این فصل می خواهیم نشان دهیم که با یک فرض پیچیدگی محاسباتی معقول که در ادامه گفته می شود بوسیله اثبات هایی به نام اثبات های طبیعی قادر به ثابت کردن $NP \not\subseteq P/poly$ نیستیم.

در حقیقت نشان می دهیم که با یک فرض معقول پیچیدگی محاسباتی ثابت کردن کران پایین برای مدارهای منطقی سخت است.

۲ اثبات های طبیعی

تعریف ۱. *فرض کنید که $f : \{0,1\}^n \rightarrow \{0,1\}$ و $c \geq 1$ باشد، اثباتی برای اینکه $f \notin \mathbf{size}(n^c)$ را می توان به وسیله یک محمول منطقی مثل φ بیان کرد به طوری که داشته باشیم:*

1. $\varphi(f)$
2. $\forall g \in \mathbf{size}(n^c) : \neg\varphi(g)$

اگر یک محمول منطقی شرط دومی که در بالا ذکر شد را داشته باشد می گوییم که آن محمول یک محمول n^c -مفید است. به محمولی که علاوه بر دو شرط بالا دو شرط زیر را نیز داشته باشد محمول طبیعی می گوییم.

۱. *ساختی بودن:*
یک ماشین تورینگ با زمان اجرای $2^{O(n)}$ وجود داشته باشد که بر روی جدول ارزش یک تابع مثل $g : \{0,1\}^n \rightarrow \{0,1\}$ به عنوان ورودی مقدار $\varphi(g)$ را محاسبه کند. دقت داشته باشید که اندازه جدول ارزش یک تابع از $O(2^n)$ می باشد، پس زمان اجرای ماشین تورینگ مذکور نسبت به طول ورودی چند جمله ای می باشد.

۲. *بزرگی:*
احتمال اینکه برای یک تابع مثل $g : \{0,1\}^n \rightarrow \{0,1\}$ داشته باشیم $\varphi(g)$ حداقل $1/n$ باشد.

نکته ای که وجود دارد اینست که شرط بزرگی با شرط n^c -مفید تناقضی ندارد، زیرا می دانیم تعداد کمی از توابع مدار با اندازه چند جمله ای دارند. حال با ذکر چند مثال به درک بهتر محمول های طبیعی می پردازیم.

مثال ۲. *محمول φ را به این صورت در نظر بگیرید که برای یک تابع مثل $g : \{0,1\}^n \rightarrow \{0,1\}$ درست است اگر و تنها اگر این تابع دارای پیچیدگی مدار بیشتر از $n^{lg(n)}$ باشد. با توجه به تعریف این محمول، این محمول برای هر $c \geq 1$ یک محمول n^c -مفید است، زیرا $n^c = O(n^{lg(n)})$. هم چنین φ خاصیت بزرگی را نیز دارد، زیرا اکثر توابع دارای اندازه مدار غیر چند جمله ای هستند، ولی ما نمی دانیم که خاصیت ساختی بودن نیز برای این محمول درست است یا خیر. یک روش بدیهی برای محاسبه مقدار φ برروی جدول ارزش تابع g محاسبه تمام مدار های با اندازه $n^{lg(n)}$ و چک کردن تساوی آن ها با تابع g است که زمان اجرا این کار $O(2^{n^{lg(n)}})$ است.*

مثال ۳. *محمول φ را به این صورت در نظر بگیرید که برای یک تابع مثل $g : \{0,1\}^n \rightarrow \{0,1\}$ درست است اگر و تنها اگر مساله $3SAT$ را برای ورودی های به اندازه n به درستی حل کند. این محمول خاصیت ساختی بودن را دارد، زیرا باتوجه به اینکه ورودی قرار است جدول ارزش تابع g باشد می توان تمام عبارت های منطقی به فرم $3CNF$ که اندازه ی آن ها n است را لیست کرد و ارضاپذیری همه ی آن ها را در زمان $2^{O(n)}$ حساب کرد و مقدار g را نیز برروی آن ها حساب کرد و به این طریق φ را حساب کرد، چون اندازه ورودی $O(2^n)$ است، پس زمان اجرای این روش نسبت به طول ورودی چند جمله ای می باشد. باید توجه داشت که n^c -مفید بودن φ یک مساله باز است. هم چنین φ خاصیت بزرگی را ندارد زیرا برای دقیقا یک تابع درست است.*

۱.۲ چرا ساختی بودن؟

ساختی بودن در ریاضیات امری بسیار مهم است تا جایی که ریاضیدانانی وجود دارند که اثبات های غیر ساختی را قبول ندارند. از لحاظ علوم کامپیوتر نیز ساختی بودن اثبات ها مهم است، زیرا وقتی وجود یک شی به صورت ساختی ثابت می

شود، یک الگوریتم برای ساخت آن شی وجود دارد، مثلا اگر به صورت ساختی ثابت شود که برای مساله SAT یک الگوریتم چند جمله ای وجود دارد، از آن اثبات می توان الگوریتم مورد نظر را استخراج کرد. باید دقت داشت که تمام احکام ریاضی به صورت ساختی قابل اثبات نیستند.

قضیه ۴. *تابع ساختی یک به یک و پوشایی مثل $f:[0,1]\rightarrow\mathbb{R}$ وجود ندارد.*

اثبات. به کتاب $Constructivisem\ in\ Mathematics$ مراجعه شود. □

این در حالی است که می دانیم چنین تابعی وجود دارد. طبق تعریف ساختی بودن اگر نشان داده شود که وجود یک شی به صورت ساختی قابل اثبات نیست، می توان فرض کرد که از چنین شی ای نمی توان استفاده کرد، برای مثال اگر نشان داده شود که برای $P=NP$ یک اثبات ساختی وجود ندارد، در عمل نیاز به عوض کردن سیستم های رمزنگاری نداریم، هر چند به صورت غیر ساختی $P=NP$ ثابت شود! نکته دیگری که ساختی بودن را مهم می کند اینست که در اکثر احکام ترکیبیاتی و کران پایین برای مدارهای منطقی اثبات های غیرساختی داشته اند، بعدا اثباتی ساختی به معنی ای که در تعریف اثبات های طبیعی ذکر شد پیدا شده است. یکی از این احکام لم محلی لواژ است که اثبات اولیه آن غیر ساختی است.

۲.۲ چرا بزرگی؟

قضیه زیر طبیعی بودن شرط بزرگی را نشان می دهد.

قضیه ۵. *هر اثباتی برای اینکه نشان دهد پیچیدگی مدار تابع $f:\{0,1\}^n\rightarrow\{0,1\}$ بیشتر از S نشان می دهد که حداقل نصف توابع n متغیره دارای پیچیدگی مدار بیشتر از $S/2-10$ هستند.*

اثبات. یک تابع دلخواه مثل $g:\{0,1\}^n\rightarrow\{0,1\}$ را در نظر بگیرید، اگر هر دو تابع g و $g\oplus f$ هر دو دارای پیچیدگی مدار کمتر از $S/2-10$ باشند، آنگاه تابع $(f\oplus g)\oplus g=f$ دارای پیچیدگی مدار کمتر مساوی S می شود که این خلاف فرض است، باتوجه به اینکه تابع g به صورت دلخواه انتخاب شده بود و با انتخاب هر تابع مثل h حداقل یکی از توابع h یا $f\oplus h$ دارای پیچیدگی مدار بیشتر از $S/2-10$ هستند، پس حداقل نصف توابع دارای پیچیدگی مدار بیشتر از $S/2-10$ می باشند. □

باتوجه با قضیه قبل داشتن شرط بزرگی معقول می باشد.

۳.۲ اثبات های طبیعی از دیدگاه اندازه های پیچیدگی

به صورت کلی اکثر روش های اثبات کران های پایین برای مدار های منطقی منجر به یک اثبات طبیعی می شوند. به طور کلی یکی از راه هایی که می توان نشان داد یک تابع پیچیده است، اینست که این موضوع را به صورت استقرایی نشان دهیم، یعنی از اینکه یک تابع پیچیده است بتوانیم نتیجه بگیریم که یکی از توابع سازنده آن پیچیده است. به طور دقیق تر یکی از راه های نشان دادن پیچیدگی تعریف یک اندازه بر روی توابع می باشد. یک تابع مثل μ از توابع n متغیره بولی به اعداد صحیح نا منفی است که دارای خواص زیر است:

$I.\forall i:\mu(x_i)+\mu(\neg x_i)\leq 2$

$II.\mu(f\wedge g)\leq\mu(f)+\mu(g)$

$III. \mu(f \vee g) \leq \mu(f) + \mu(g)$

را اندازه فرمال می گوییم.

بَرای اندازه های فرمال قضیه زیر را داریم:

قضیه ۶. *برای هر اندازه فرمال μ، $\mu(f)$ یک کران پایین برروی پیچیدگی فرمول تابع f است.*

اثبات. به وسیله استقرای ریاضی. □

برای اینکه بتوانیم ار اندازه فرمال بهره ببریم، مثلا ثابت کنیم که مساله SAT دارای پیچیدگی مدار نمایی است، باید اندازه فرمالی تعریف کنیم که برای همه توابع چند جمله ای مقدار کمتری نسبت به تابع محاسبه کننده مساله SAT داشته باشد، اما باید دقت داشت تعریف چنین اندازه ای موجب به دست آوردن کران پایین برای توابع دیگری هم می شود، به طور دقیق تر داریم:

قضیه ۷. *اگر μ یک اندازه فرمال باشد و برای تابع $f : \{۰,۱\}^n \to \{۰,۱\}$ داشته باشیم $\mu(f) \geq S$ آنگاه حداقل برای ۱/۴ توابع n متغیره مثل g داریم، $\mu(g) \geq S/۴$.*

اثبات. مثل اثبات قضیه ۵ یک تابع n متغیره دلخواه مثل g را در نظر می گیریم و داریم، f=(f $\oplus g) \oplus g$ ، پس داریم، $f = (\neg(f \oplus g) \wedge g) \vee ((f \oplus g) \wedge \neg g)$. حال اگر $h = f \oplus g$ باشد، داریم، $\mu(f) \leq \mu(h) + \mu(\neg h) + \mu(g) + \mu(\neg g)$. اگر همه ۴ اندازه ای که باهم جمع کرده ایم کمتر از $S/۴$ باشد، آنگاه $\mu(f) < S$ که این با فرض تناقض دارد، پس حداقل یکی از توابع مذکور دارای اندازه بیشتر مساوی $S/۴$ است، چون تابع g را به دلخواه انتخاب کرده بودیم پس برای حداقل ۱/۴ توابع مثل w داریم، $\mu(w) \geq S/۴$. □

حال به اثبات مهم ترین قضیه این فصل می رسیم.

قضیه ۸. *اگر یک تابع یک طرفه قوی زیرنمایی وجود داشته باشد، آنگاه عدد طبیعی c وجود دارد که هیچ محمول منطقی n^c - مفید وجود ندارد.*

اثبات. فرض کنید تابع قوی یک طرفه ما به نام f، تابعی باشد که برای یک $۰ < \epsilon$ مشخص و ثابت خروجی اش با هیچ الگوریتم تصادفی بازمان اجرای ۲^{n^ϵ} قابل وارون کردن نباشد. طبق قضیه می دانیم به وسیله این تابع می توان یک خانواده از توابع سودو رندوم جنریتور مثل $\{f_s\}_{s\in\{۰,۱\}^*}$ که دارای درجه امنیت ۲^{m^β} برای یک β مشخص هستند، ساخت. در نتیجه این خانواده از توابع این خاصیت را دارند که الگوریتم با زمان اجرای چندجمله ای وجود دارد که با گرفتن s و x مقدار $f_s(x)$ را محاسبه می کند. هم چنین هیچ الگوریتم با زمان اجرای ۲^{m^β} برای تشخیص $f_s(.)$ برای $s \in \{۰,۱\}^m$ از یک تابع تصادفی وجود ندارد. حال برای رسیدن به تناقض فرض کنید که یک محمول منطقی طبیعی مثل φ داریم که n^c -مفید برای یک c مشخص که در ادامه معرفی می شود، نیز است. حال الگوریتمی با زمان مناسب طراحی می کنیم که با احتمال خوبی خانواده سودو رندوم جنریتور را از توابع تصادفی تشخیص دهد. به این صورت عمل می کنیم که با گرفتن یک تابع تصادفی مثل h جدول ارزش تابع $g(x) = h(x ۰^{m-n})$ را که از $\{۰,۱\}^n$ به $\{۰,۱\}$ که $n = m^{\beta/۲}$ است را می سازیم. زمان اجرای اینکار $۲^{O(n)}$ می باشد. حال محمول φ را برروی این تابع اجرا می کنیم و خروجی آن را به عنوان خروجی الگوریتم می دهیم. حال دو اتفاق ممکن است رخ دهد: اول اینکه تابع h یک تابع تصادفی است که در نتیجه آن تابع g نیز یک تابع تصادفی می شود که طبق تعریف محمول طبیعی به احتمال حداقل $۱/n$ داریم $\varphi(g)$ ، دوم اینکه تابع h یکی از توابع خانواده مذکور مثل f_s برای یک s خاص باشد که از آن جایی که این توابع در زمان چندجمله ای قابل محاسبه هستند پس مدار های آن ها برای یک c مناسب دارای اندازه حداکثر n^c می شوند، در نتیجه طبق تعریف داریم $\neg\varphi(g)$. پس این الگوریتم ارائه شده بین یک تابع تصادفی و یک تابع از خانواده توابع مذکور با احتمال حداقل $۱/n$ تفاوت قائل می شود، از طرفی زمان اجرای این الگوریتم $۲^{O(n)}$ است

که کمتر از 2^{m^β} می باشد که این خلاف درجه امنیت خانواده توابعی که داشتیم می باشد، از این تناقض به دست آمده حکم ثابت می شود. □

نتیجه ۹. *اگر یک تابع یک طرفه قوی زیرنمایی وجود داشته باشد، آنگاه هر اثباتی برای $NP \nsubseteq P/poly$ طبیعی نیست.*

اثبات. باتوجه به قضیه ۸ واضح می باشد. □