دانشگاه صنعتی شریف

عنوان:

سمینار درس پیچیدگی محاسباتی

Proof Complexity

استاد راهنما: جناب آقای دکتر فروغمند

تهیه کننده: زهرا علیزاده

۹۳۳۰۱۰۳۵

بهار ۱۳۹۴

چکیده:

در این سمینار روی یکی از بنیادی‌ترین موضوعات مطرح شده در پیچیدگی محاسبه که بررسی مفهوم دستگاه اثبات می‌باشد تمرکز شده است. دستگاه اثبات مربوط به یک مسئله، الگوریتمی است که یک نمونه از آن مسئله را به همراه یک اثبات دریافت کرده و درستی اثبات ارائه شده را برای آن نمونه از مسئله بررسی می‌کند. در مطالب جمع‌آوری شده در این تحقیق به طور ویژه مسائلی مورد بررسی قرار می‌گیرند که از نظر شهودی وجود اثباتی با طول چندجمله‌ای برای برخی از نمونه‌های آن مسائل امکان‌پذیر نمی‌باشد. در ادامه این ارائه به معرفی و بررسی چند دستگاه اثبات می‌پردازیم که می‌توان نشان داد برای اکثر این دستگاه‌ها نمونه مسئله‌هایی وجود دارند که کران پایین طول اثبات ارائه شده برای این نمونه مسئله‌ها نمایی می‌باشد. برای یک مسئله coNP-تمام مانند $\overline{\mathrm{SAT}}$ اگر دستگاه اثباتی وجود داشته باشد که بتوان نشان داد اثبات‌های ارائه شده برای تمام نمونه‌های این مسئله در این دستگاه دارای طول چندجمله‌ای است، آنگاه نشان داده‌ایم NP=coNP؛ اما به طور شهودی چنین نتیجه‌ای نادرست به نظر می‌رسد.

مقدمه:

در تعریف رده پیچیدگی NP به دنبال مجموعه زبان‌هایی بودیم که می‌توانستیم برای آنها یک الگوریتم چندجمله‌ای ارائه دهیم که برای هر نمونه از مسئله داده شده با گرفتن این نمونه و نیز با دریافت یک سند باطول چندجمله‌ای می‌توانستیم عضویت این نمونه را در زبان داده شده اثبات کنیم. به عبارتی زبان L متعلق به رده پیچیدگی NP است اگر یک تصدیق‌گر V با زمان اجرای چندجمله‌ای و نیز یک چندجمله‌ای P وجود داشته باشد بطوریکه داشته باشیم:

$$x \in L \iff \exists y \quad |y| \leq P(|x|) \quad V(x,y) = 1$$

اما با توجه به حدس NP≠co-NP به طور شهودی به نظر می‌رسد برای مسائل co-NP نمی‌توان چنین تصدیق‌گری داشت که بتواند با استفاده از سند با طول چندجمله‌ای عضویت یک عضو از زبان را تصدیق کند.

با تعمیم تعریف ارائه شده برای مسائل NP، یک دستگاه اثبات به شکل زیر تعریف می‌شود:

یک دستگاه اثبات برای زبان L یک تصدیق گر V با زمان اجرای چندجمله‌ای است بطوریکه داشته باشیم:

$$x \in L \Leftrightarrow \exists y \quad V(x ,y) = 1$$

که تصدیق‌گر V باید نسبت به طول هر دو ورودی x و y دارای زمان اجرای چندجمله‌ای باشد. همانطور که ملاحظه می‌کنید هیچ محدودیتی روی طول سند (اثبات) ارائه شده، y، وجود ندارد. در این تعریف، کوتاه‌ترین طول ممکن برای اثبات، رده پیچیدگی دستگاه اثبات مربوطه را تعیین می‌کند. لذا یک زبان در NP است اگر و تنها اگر دستگاه اثباتی با رده پیچیدگی چندجمله‌ای برای آن موجود باشد. اما مسائلی وجود دارند که بدون هیچ قید و شرطی می‌توان نشان داد هیچ دستگاه اثبات چندجمله‌ای برای آنها وجود ندارد. برای مثال می‌توان با استفاده از قطری‌سازی نشان داد که زبان‌هایی خارج از رده co-NP وجود دارند و همین زبان‌ها را به عنوان زبان‌های فاقد دستگاه اثبات چندجمله‌ای در نظر گرفت. از طرفی طبق اصل ناتمامیت گودل، یک زبان شناخته شده وجود دارد که با اطمینان می‌توان گفت هیچ سند متناهی برای آن وجود ندارد. این زبان شامل تمام گزاره‌های درست روی اعداد طبیعی در منطق مرتبه اول می‌باشد. در صورتی که بتوان دستگاه اثباتی برای آن داشت که طول سندها در آن متناهی باشد، آنگاه می‌توان مسئله توقف را حل کرد؛ در حالی که می‌دانیم این مسئله تصمیم‌ناپذیر است.

در ادامه چند مثال ارائه می‌کنیم که به طور شهودی نمی‌توانند دارای دستگاه اثبات با پیچیدگی چندجمله‌ای باشند اما برای برخی از آنها می‌توان نشان داد که چنین دستگاه اثباتی وجود دارد.

۱.دستگاه‌های نامعادلات خطی فاقد جواب:

یک دستگاه از نامعادلات خطی به شکل زیر داده شده است که در آن $\boldsymbol{a}_i$ برداری حقیقی و n-بعدی بوده و b_i عددی حقیقی است و هدف مسئله این است که اثباتی ارائه دهیم که نشان دهد هیچ بردار حقیقی نامنفی وجود ندارد که در همه این نامعادلات صدق کند.

$$\langle \boldsymbol{a_1}, \boldsymbol{x} \rangle \leq b_1$$
$$\langle \boldsymbol{a_2}, \boldsymbol{x} \rangle \leq b_2$$
$$\vdots$$
$$\langle \boldsymbol{a_m}, \boldsymbol{x} \rangle \leq b_m$$

به نظر می‌رسد نتوانیم برای نمونه‌هایی که عضو این مسئله هستند اثباتی با طول چندجمله‌ای ارائه دهیم؛ اما طبق لم فارکاس، می‌توان نشان داد که این شهود اشتباه است: دستگاه فوق فاقد جواب است اگر و تنها اگر یک ترکیب خطی از نامعادلات آن وجود داشته باشد که ما را به یک تناقض بدیهی برساند. به عبارتی به دنبال یک بردار $\boldsymbol{y} \in R^m$ هستیم که حاصل $\sum_{i=1}^{n} y_i a_i$ نامنفی بوده و از طرفی نیز داشته باشیم $\sum_i y_i b_i < 0$.

۲.دستگاه‌های معادلات چندجمله‌ای فاقد جواب:

یک دستگاه از چندجمله‌ای‌های $g_1(x_1, x_2, \ldots, x_n)$ ، $g_2(x_1, x_2, \ldots, x_n)$ ، ... و $g_m(x_1, x_2, \ldots, x_n)$ با ضرایب حقیقی داده شده است. به دنبال سندی هستیم که نشان دهد دستگاه فوق دارای هیچ جواب مشترکی نمی‌باشد.

۳.مجموعه عبارات منطقی ارضاناپذیر:

فرض کنید یک فرمول منطقی φ داده شده است. به دنبال ارائه سندی هستیم که نشان دهد هیچ مقداردهی ارضاکننده‌ای برای فرمول داده شده وجود ندارد.

دستگاه اثبات گزاره‌ای:

دستگاه اثبات گزاره‌ای، دستگاه اثبات V برای مجموعه تاتولوژی‌های منطق گزاره‌ای می‌باشد به طوری که داشته باشیم:

$$\varphi \in TAUT \Leftrightarrow \exists\, proof\ y \quad V(x,y)=1$$

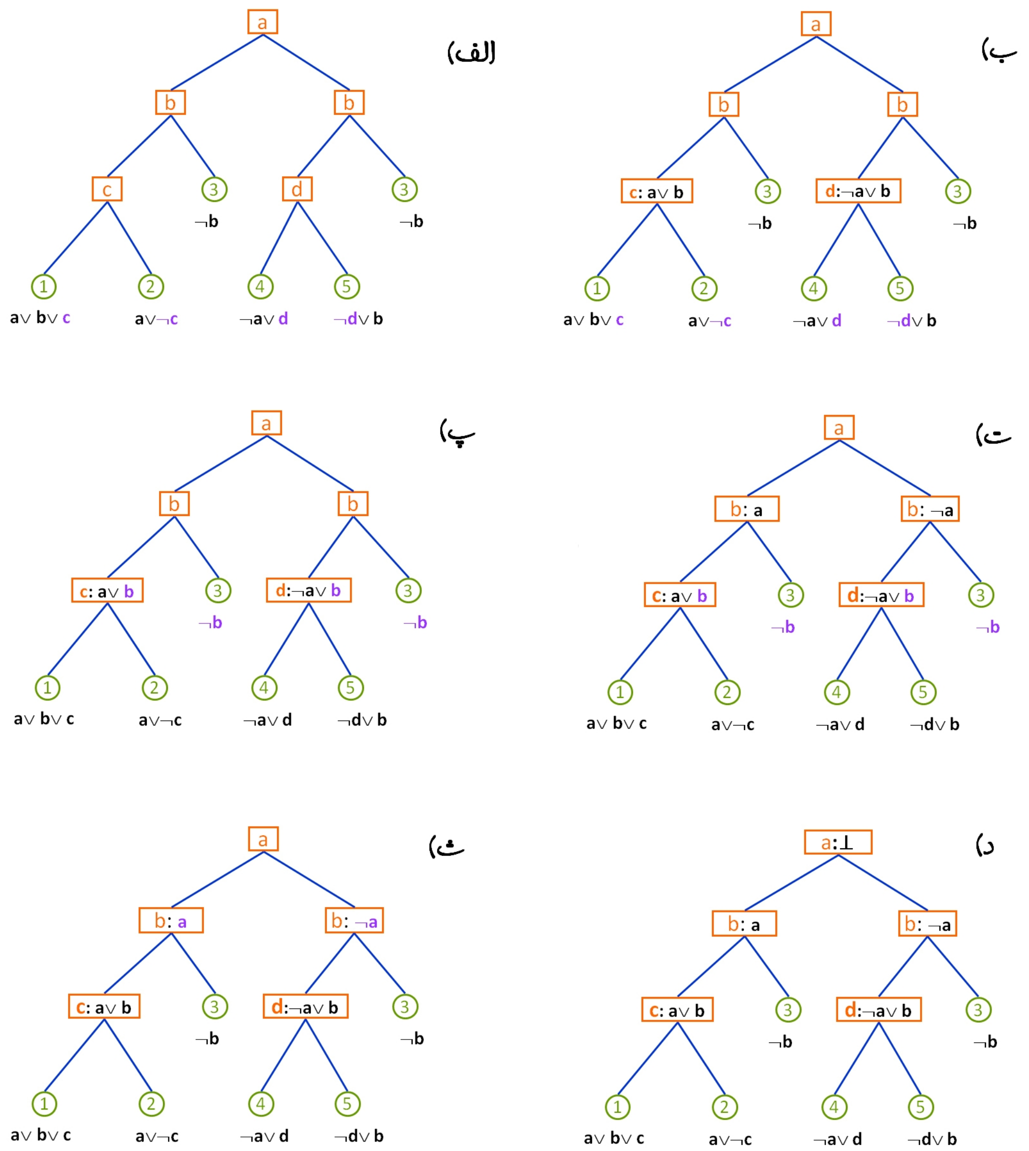
اما از آنجاییکه مجموعه تاتولوژی‌های منطق گزاره‌ای برابر است با نقیض مجموعه گزاره‌های ارضاناپذیر در منطق گزاره‌ای، لذا می‌توان دستگاه اثبات گزاره‌ای را به شکل یک دستگاه اثبات V برای مجموعه $UNSAT$ شامل گزاره‌های ارضاناپذیر تعریف کرد به طوری که داشته باشیم:

$$\varphi \in UNSAT \Leftrightarrow \exists\, proof\ y \quad V(x,y)=1$$

دستگاه اثبات Resolution:

در این بخش یک فرآیند ساده معرفی می‌کنیم که هدف آن تولید اثباتی است که نشان دهد یک فرمول داده شده ارضاناپذیر است. فرض می‌کنیم فرمول φ با فرم CNF داده شده است که دارای m کلاز c_1 تا c_m می‌باشد. برای $j=m+1, m+2, \ldots$ کلاز c_j را با استفاده از مجموعه کلازهای c_1 تا c_{j-1} به این شکل می‌سازیم که اگر هر دو کلاز $x_i \vee C$ و $\neg x_i \vee D$ در مجموعه فوق وجود داشته باشد آنگاه خواهیم داشت $c_j = C \vee D$. البته ممکن است در هر زمانی چندین انتخاب برای c_j داشته باشیم اما به هر حال اثبات به دست آمده مجموعه‌ای از این انتخاب‌ها می‌باشد. واضح است که هر کلاز به دست آمده نتیجه منطقی کلازهای موجود می‌باشد. اما این فرآیند تا جایی ادامه پیدا می‌کند که به یک تناقض واضح و بدیهی برسیم که این تناقض زمانی به دست می‌آید که دو کلاز به شکل x_i و $\neg x_i$ برای یک متغیر x_i در این دنباله از Resolution ظاهر شود. در این حالت می‌گوییم Refutation اتفاق افتاده است. برای مثال مجموعه کلازهای زیر را در نظر بگیرید که در شکل۱، Resolution مربوط به آن به شکل درخت نشان داده شده است.

$a \vee b \vee c,\ \ a \vee \neg c,\ \ \neg b,\ \ \neg a \vee d,\ \ \neg d \vee b$



شکل۱: مراحل به دست آوردن یک Refutation برای ۵ کلاز داده شده که با شروع از شکل الف در ۶ مرحله انجام می‌پذیرد

در ادامه نشان می‌دهیم فرمول‌هایی در مجموعه فرمول‌های ارضاناپذیر وجود دارند که کران پایین طول اثبات آن‌ها در این دستگاه اثبات گزاره‌ای، نسبت به طول فرمول ورودی φ نمایی می‌باشد. این کار را با استفاده از اصل لانه کبوتری انجام می‌دهیم. طبق اصل لانه کبوتری هیچ نگاشت یک به یک و پوشایی از یک مجموعه m عضوی به یک مجموعه n عضوی با شرط $m>n$ وجود ندارد. اما اگر بخواهیم این اصل را به صورت گزاره‌ای بیان کنیم، به مجموعه فرمول‌های CNF به شکل $\{\neg PHP_n^m \quad m>n\}$ می‌رسیم. برای تعریف فرمول‌های این مجموعه، ابتدا متغیرهای بولی P_{ij} را به ازای $i\le m$ و $j\le n$ به این شکل تعریف می‌کنیم که P_{ij} را تنها در صورتی

برابر با true در نظر می‌گیریم که کبوتر i ام به لانه j ام برود. هر فرمول شامل دو دسته کلاز به شکل زیر می‌باشد:

۱.برای هر $i\leq m$ کلازی به شکل $(P_{i1} \vee P_{i2} \vee \ldots \vee P_{in})$ تعریف می‌کنیم که تضمین می‌کند حتما یکی از لانه‌ها به i امین کبوتر اختصاص یافته است.

۲.برای هر $i,j\leq m$ و $k\leq n$ کلازی به شکل $(\neg P_{ik} \vee \neg P_{jk})$ داریم که تضمین می‌کند k امین لانه نمی‌تواند به طور همزمان به دوکبوتر i و j اختصاص یافته باشد.

با عطف مجموعه این کلازها می‌توانیم تضمین کنیم که هریک از لانه‌ها دقیقا به یک کبوتر اختصاص یافته است و نیز کبوتری وجود ندارد که لانه‌ای به آن اختصاص نیافته باشد. اگر $\neg P_{ij}$ را معادل با $\vee_{l\neq i} P_{lj}$ در نظر بگیریم و در فرمول حاصل از *Resolution* جایگزین کنیم، آنگاه به یک فرمول یکنواخت، یعنی فرمولی که هیچ لیترال با علامت نقیض در آن وجود ندارد، می‌رسیم که با فرمول اولیه معادل است. اگر قضیه زیر را اثبات کنیم آنگاه نشان داده‌ایم که در دستگاه اثبات *Resolution* نمونه‌هایی وجود دارند که طول *Resolution* آنها نسبت به طول نمونه ورودی نمایی می‌باشد.

قضیه: به ازای هر $n\geq 2$ ، هر Resolution Refutation برای $\neg PHP^{n}_{n-1}$ دارای حداقل اندازه $2^{n/20}$ می‌باشد.

اما برای اثبات قضیه فوق از لم زیر استفاده می‌کنیم:

لم: هر Resolution Refutation یکنواخت برای $\neg PHP^{n}_{n-1}$ باید شامل یک کلاز با حداقل تعداد $2n^2/9$ متغیر باشد.

اثبات: برای اثبات این لم ابتدا مقداردهی بحرانی را تعریف می‌کنیم. برای اختصاص n-1 لانه به n کبوتر، قطعا باید n-1 کبوتر را به n-1 لانه نگاشت کنیم و یکی از کبوترها بدون لانه باقی می‌ماند. به عبارت دیگر یک

مقداردهی برای P_{ij}ها به دست می‌آید. یک مقداردهی را k-بحرانی می‌نامیم اگر کبوتری که در این مقداردهی لانه‌ای به آن اختصاص نیافته است، k امین کبوتر باشد.

برای هر کلاز C در Refutation یکنواخت، مجموعه $witness(C)$ را به شکل زیر تعریف می‌کنیم:

$witness(C)$ = { i : یک مقداردهی i-بحرانی α وجود دارد که کلاز C را false می‌کند }

پیچیدگی کلاز C را با نماد $comp(C)$ نشان می‌دهیم و آن را برابر با تعداد اعضای مجموعه $witness(C)$ در نظر می‌گیریم. هرگاه قاعده Resolution برای به دست آوردن کلاز C از روی دو کلاز C' و C'' مورد استفاده قرار بگیرد، آنگاه داریم: $comp(C) \leq comp(C')+comp(C'')$، زیرا با توجه به قاعده Resolution، هر مقداردهی که کلاز C را $false$ کند باید حداقل یکی از کلازهای C' و C'' را $false$ کند. بنابراین اگر C اولین کلازی در Refutation باشد که پیچیدگی آن بزرگتر از $n/3$ می‌باشد، آنگاه نتیجه می‌شود: $n/3<comp(C)<2n/3$. باید نشان دهیم که چنین کلازی یک کلاز بزرگ است. به طور خاص ثابت می‌کنیم که اگر $comp(C)=t$ باشد، آنگاه شامل حداقل $t(n-t)$ لیترال مجزا می‌باشد. لذا با توجه به رابطه $t(n-t)>2n^2/9$، لم اثبات می‌شود.

یک اندیس $i \in witness(C)$ را به همراه یک مقداردهی i-بحرانی α که کلاز C را false می‌کند انتخاب می‌کنیم. برای هر $j \notin witness(C)$، مقداردهی j-بحرانی α' را از روی مقداردهی α و با تبادل i و j به این شکل به دست می‌آوریم که اگر در مقداردهی α، کبوتر j به لانه l می‌رود، آنگاه مقداردهی α'، کبوتر i را به لانه l می‌نگارد و به کبوتر j هیچ لانه‌ای را اختصاص نمی‌دهد. اما از آنجاییکه $j \notin witness(C)$، لذا این مقداردهی j-بحرانی باید کلاز C را ارضا کند. لذا کلاز C باید شامل متغیر P_{il} باشد که بتواند دقیقا با اختصاص دادن کبوتر i به لانه l ارضا شود. لذا اگر همین کار را با استفاده از مقداردهی α روی همه $n-t$ اندیس $j \notin witness(C)$ انجام دهیم، آنگاه به وضوح نتیجه می‌شود که C شامل $n-t$ متغیر P_{il} می‌باشد. اگر کل فرآیند فوق را برای هر $i \in witness(C)$ ، انجام دهیم، نتیجه می‌گیریم که C شامل حداقل $t(n-t)$ متغیر می‌باشد و لم اثبات می‌شود.

با استفاده از لم فوق، اثبات قضیه اصلی به شرح زیر می‌باشد:

یک کلاز را در Refutation یکنواخت، بزرگ می‌گوییم اگر حداقل به تعداد $n^2/10$ متغیر داشته باشد. اگر L را برابر با تعداد کلازهای بزرگ در نظر بگیریم، آنگاه طبق لم فوق $L\geq 1$ می‌باشد. میانگین‌ها نشان می‌دهند که متغیر P_{ij} وجود دارد که در تعداد حداقل 1/10 از کلازهای بزرگ ظاهر می‌شود. اگر برای این متغیر قرار دهیم $P_{ij}=1$ و همچنین به ازای هر $j'\neq j$ و نیز به ازای هر $i'\neq i$ قرار می‌دهیم $P_{ij'}=0$ و $P_{i'j}=0$، با این مقداردهی در واقع تمام کلازهایی که شامل متغیر P_{ij} هستند ارضا می‌شوند و می‌توانیم آنها را حذف کنیم. به عبارتی حداکثر به تعداد $9/10L$ کلاز بزرگ باقی می‌ماند. علاوه‌براین، با این مقداردهی در واقع یک کبوتر و یک لانه از لیست موجود حذف می‌شوند. لذا یک اثبات Refutation یکنواخت برای $\neg PHP_{n-2}^{n-1}$ خواهیم داشت. اگر گام فوق را به تعداد $t=\log_{10/9}L$ بار انجام دهیم، آنگاه یک اثبات Refutation یکنواخت برای $\neg PHP_{n-t-1}^{n-t}$ به دست می‌آوریم که هیچ کلاز بزرگی در آن وجود ندارد. اگر $L<2^{n/20}$ باشد، آنگاه $t<n/3$ خواهد بود و لذا یک Refutation یکنواخت برای فرمول $\neg PHP_{n-t-1}^{n-t}$ خواهیم داشت که هیچ کلازی بزرگتر از $n^2/10$ ندارد که این عدد کوچکتر از $2(n-t)^2/9$ می‌باشد و این با لم قبل متناقض می‌باشد. لذا قضیه اثبات می‌شود و ما به یک کران پایین نمایی برای دستگاه اثبات گزاره‌ای می‌رسیم.

چند دستگاه اثبات دیگر:

در این بخش چند دستگاه اثبات دیگر را به طور مختصر معرفی می‌کنیم که برای برخی از آنها کران پایین نمایی اثبات شده است ولی برای برخی از دستگاه‌های قوی‌تر، در حال حاضر هیچ کران پایین نمایی اثبات نشده است.

صفحه‌های برشی:

این دستگاه اثبات برای مسئله تصدیق فاقد جواب بودن یک مجموعه از نامعادلات خطی با ضرایب و متغیرهای صحیح مورد استفاده قرار می‌گیرد. این مسئله co-NP-تمام است. لذا می‌توان هر فرمول φ با فرم CNF را به یک نمونه از چنین مجموعه‌ای تبدیل کرد به طوری که فرمول داده شده ارضاناپذیر باشد اگر و تنها اگر این

مجموعه از نامعادلات فاقد جواب باشد. برای این منظور، متناظر با هر متغیر x_i در فرمول φ، یک متغیر صحیح X_i با شرط $0\leq X_i\leq 1$ (به عبارتی $X_i \in \{0,1\}$) قرار می‌دهیم. برای یک کلاز $x_i \vee x_j \vee x_k$ یک نامعادله به شکل $x_i + x_j + x_k \geq 1$ قرار می‌دهیم. اگر هر متغیر x_i به صورت منفی ظاهر شده باشد، آنگاه در نامعادله فوق، به جای آن متغیر، $(1\text{-}x_i)$ را قرار می‌دهیم.

این دستگاه اثبات شامل فرآیندی است که برای یک مجموعه از نامعادلات خطی فاقد جواب، یک اثبات برای عدم وجود جواب ارائه می‌دهد که به شکل دنباله‌ای از نامعادلات $l_1 \geq 0,\ l_2 \geq 0, \ldots, l_T \geq 0$ می‌باشد که r امین نامعادله از این دنباله، در یکی از سه دسته زیر جای می‌گیرد:

۱.یکی از نامعادلات ظاهر شده در دستگاه خطی داده شده می‌باشد.

۲.برابر با $\alpha l_u+\beta l_v\geq 0$ می‌باشد به طوری که α و β اعداد صحیح نامنفی بوده $u,v<r$ می‌باشد.

۳.از روی یک l_u که $u<r$ بوده و با اعمال این قاعده به دست می‌آید که اگر l_u به شکل $\sum_{i=1}^{n} a_i x_i - b \geq 0$ باشد که بزرگترین مقسوم‌علیه مشترک اعداد a_1 تا a_n برابر با $D\geq 2$ می‌باشد، در این صورت نامعادله جدید به شکل $\sum_{i=1}^{n} \frac{a_i}{D} x_i - \left\lceil \frac{b}{D} \right\rceil \geq 0$ خواهد بود.

برای دستگاه اثبات صفحه‌های برشی، کران پایین نمایی اثبات شده است. یعنی نمونه‌هایی از این مسئله وجود دارند که طول اثبات تولید شده با این دستگاه اثبات برای آنها نمایی می‌باشد. مثال ارائه شده در شکل۲ نشان می‌دهد که می‌توان با استفاده از قواعد موجود در این دستگاه، قاعده Resolution را به دست آورد.

Resolution: $\dfrac{(a \vee b \vee c \vee \neg d) \quad (\neg a \vee b \vee c \vee \neg r)}{(b \vee c \vee \neg d \vee \neg r)}$

Cutting Planes:
$$\begin{array}{l} a + b + c + (1\text{-}d) \geq 1 \\ (1\text{-}a) + b + c + (1\text{-}r) \geq 1 \\ (1\text{-}d) \geq 0 \\ (1\text{-}r) \geq 0 \\ \hline 2b + 2c + 2(1\text{-}d) + 2(1\text{-}r) \geq 1 \\ \hline b + c + (1\text{-}d) + (1\text{-}r) \geq 1 \end{array}$$

شکل۲: تولید قاعده Resolution با استفاده از قواعد موجود در دستگاه صفحات برشی

محاسبات چندجمله‌ای:

این دستگاه اثبات برای مسئله تصدیق فاقد جواب بودن یک مجموعه از معادلات چندجمله‌ای مورد استفاده قرار می‌گیرد. فرض می‌کنیم مجموعه معادلات چندجمله‌ای به شکل زیر داده شده است:

$$P_1(x_1, x_2, \ldots, x_n) = 0$$
$$\vdots$$
$$P_m(x_1, x_2, \ldots, x_n) = 0$$

نکته قابل توجه اینجاست که ارضاناپذیر بودن فرمول‌های 3CNF را با استفاده از این دستگاه نیز می‌توان اثبات کرد. برای هر متغیر x_i در فرمول 3CNF یک متغیر X_i و یک معادله به شکل $X_i^2\text{-}X_i=0$ در نظر می‌گیریم که این اطمینان را به ما می‌دهد هر پاسخی شرط $X_i \in \{0,1\}$ را ارضا می‌کند. سپس هر کلاز را به یک معادله درجه ۳ تبدیل می‌کنیم. برای مثال معادله متناظر با کلاز $(x_i \vee x_j \vee \overline{x_k})$، به شکل $(1\text{-}X_i)(1\text{-}X_j)X_k=0$ خواهد بود.

این دستگاه اثبات، دنباله چندجمله‌ای‌های f_1 تا f_t را به گونه‌ای تولید می‌کند که هر f_r در این دنباله در یکی از سه دسته زیر جای می‌گیرد:

۱.یکی از چندجمله‌ای‌های ورودی است.

۲.یک چندجمله‌ای به شکل $\alpha f_u+\beta f_v$ می‌باشد به طوری که α و β اعداد ثابتی بوده و $u,v<r$ می‌باشد.

۳.یک چندجمله‌ای به شکل $x_i f_u$ است که x_i یک متغیر بوده و $u<r$ می‌باشد.

قواعد فوق را تا جایی اعمال می‌کنیم که به یک تناقض بدیهی برسیم. این تناقض از قضیه هیلبرت نتیجه می‌شود: یک مجموعه از معادلات $P_1(x_1,x_2, \ldots , x_n) = 0$ ، … و $P_m(x_1,x_2, \ldots , x_n) = 0$ در میدان F فاقد جواب است اگر و تنها اگر چندجمله‌ای‌های g_1، g_2، … و g_m وجود داشته باشند به طوری که داشته باشیم:

$$\sum_i g_i(x_1,\ldots,x_n)p_i(x_1,\ldots,x_n) = 1$$

وجود g_i ها نشان می‌دهد که هیچ مقداردهی برای متغیرهای x_1 تا x_n نمی‌تواند نامعادلات چندجمله‌ای P_1 تا P_m را صفر کند. زیرا در صورت وجود این مقداردهی، ترکیب فوق مارا به تناقض بدیهی $0=1$ می‌رساند. با کمی دقت می‌توان ملاحظه نمود که استفاده از سه قاعده ذکر شده برای تولید دنباله چندجمله‌ای‌ها، چندجمله‌ای‌های g_i را به طور ضمنی برای ما ایجاد می‌کند. (در واقع این عملیات، ترکیبی را به دست می‌دهد که با استفاده از آن به تناقض می‌رسیم.)

مثال ارائه شده در شکل۳ نشان می‌دهد که با استفاده از قواعد موجود در این دستگاه نیز می‌توان قاعده Resolution را به دست آورد. برای این دستگاه اثبات نیز کران پایین نمایی اثبات شده است. یعنی نمونه‌هایی از این مسئله وجود دارند که طول اثبات تولید شده با این دستگاه اثبات برای آنها نمایی می‌باشد.

Resolution: $\dfrac{(a\vee b\vee c\vee\neg d)\ (\neg a\vee b\vee c\vee\neg r)}{(b\vee c\vee\neg d\vee\neg r)}$

Polynomial Calculus: Given $a'b'c'd$ and $ab'c'r$

Derive $(a'b'c'd)r+(ab'c'r)d$

$= (a'+a)\, b'c'd\, r$

$= b'c'd\, r$

شکل۳ : تولید قاعده Resolution با استفاده از قواعد موجود در دستگاه محاسبات چندجمله‌ای

دستگاه اثبات Frege:

این دستگاه، یک دستگاه استدلال کلی‌تر در منطق گزاره‌ها است که با استفاده از تعداد متناهی از اصول موضوعه و قواعد استنتاج، به دنبال ارائه یک اثبات برای عدم درستی یک فرمول در این منطق می‌باشد. دستگاه اثبات Resolution یک حالت خاص است که تمام فرمول‌ها به شکل CNF هستند و نیز تنها یک قاعده در آن مورد استفاده قرار می‌گیرد. اما همان‌طور که ملاحظه می‌شود، این دستگاه قوی‌تر از دستگاه‌های قبلی به نظر می‌رسد و تاکنون هیچ کران پایین نمایی برای آن اثبات نشده است.

خلاصه مطالب بیان شده:

مباحث مربوط به پیچیدگی اثبات به ما این امکان را می‌دهد که برای مجموعه فرمول‌های تاتولوژی در دستگاه‌های اثبات مختلف، کران پایین ارائه کنیم. اگر $NP \neq co\text{-}NP$ باشد آنگاه برای هر اثبات کامل و نیز برای هر دستگاه اثباتی که در زمان چندجمله‌ای کار می‌کند باید فرمول‌هایی در مجموعه تاتولوژی‌ها وجود داشته باشد که نمی‌توانند دارای اثبات با طول چندجمله‌ای باشند. اما اگر برای دستگاه‌های اثبات موجود بتوان ثابت کرد که کران پایین طول اثبات آنها نمایی است، باز هم نمی‌توان لزوما ادعا کرد که $NP \neq co\text{-}NP$ برقرار است. زیرا ممکن است دستگاه قوی‌تری ارائه شود که با ارائه اثباتی با طول چندجمله‌ای برای همه نمونه‌های مسئله $\overline{SAT}$، رابطه فوق را نقض کند. همان طور که اشاره شد برای برخی از دستگاه‌های اثبات مانند محاسبات چندجمله‌ای و صفحات برشی، کران پایین با اندازه نمایی برای طول اثبات برخی از فرمول‌های تاتولوژی در این دستگاه‌ها اثبات شده است. اما در حال حاضر برای دستگاه اثبات Frege که دستگاه اثبات قوی‌تری نسبت به دستگاه‌های دیگر می‌باشد، هیچ کران پایین نمایی اثبات نشده است.