دانشگاه صنعتی شریف

دانشکده علوم ریاضی

پیچیدگی محاسبات

گزارش پایانی

تهیه کننده:

فاطمه نویدی 89109673

تابستان 94

1. مقدمه

زمانی که الگوریتم‌های تصادفی و روش‌های احتمالاتی[1] مطرح شدند برای بسیاری از مسائل راه‌حل‌های سریع با احتمال صحیح جواب دادن بالا مطرح شد این تصور ایجاد شد که تصادفی‌سازی ابزاری است که می تواند راه‌حل‌های مؤثر برای مسائلی که جواب چندجمله‌ای ندارند پیدا کند و در نتیجه $P \nsubseteq BPP$. ولی در سال‌های اخیر روش‌هایی ارائه شد که تحت فرضیات خاصی می توانند الگوریتم‌های تصادفی را قطعی‌سازی[2] کنند. با توجه به این که طبق حدس بسیاری از متخصصان این حوزه این فرضیات صحیح هستند، امروزه باور عمومی بر این است که $P = BPP$. در این ارائه به بیان این روش‌ها و فرضیات می‌پردازیم و به عنوان ابزار اصلیمان در این راه تولیدکننده‌های شبه‌تصادفی[3] را معرفی می‌کنیم.

2. تولیدکننده‌های شبه‌تصادفی در قطعی‌سازی

تعریف 1. یک توزیع R روی $\{0,1\}^n$ را برای $S \in \mathbb{N}$ و $\epsilon > 0$ یک (S,ϵ)- شبه‌تصادفی می‌گوییم اگر برای هر مدار C که اندازه‌ی آن حداکثر S است داشته‌باشیم:

$$|\Pr[C(R) = 1] - \Pr[C(U_m) = 1]| < \epsilon$$

در حالی که U_m نشان‌دهنده‌ی توزیع یکنواخت روی $\{0,1\}^n$ می‌باشد.

تعریف 2. فرض کنید $S : \mathbb{N} \to \mathbb{N}$ یک تابع باشد. یک تابع محاسبه‌پذیر در زمان 2^n مانند $G : \{0,1\}^* \to \{0,1\}^*$ را یک $S(l)$- تولیدکننده‌ی شبه‌تصادفی گوییم اگر برای هر $z \in \{0,1\}^*$، $|G(z)| = S(|z|)$ و برای هر $l \in \mathbb{N}$ توزیع $G(U_l)$ یک $(S(l)^3, {}^1\!/_{10})$- شبه‌تصادفی باشد.

در این نوشتار همواره فرض می‌کنیم تابع S یک تابع قابل ساخت زمانی[4] و غیرکاهنده است.

لم 1. فرض کنید یک $S(l)$- تولیدکننده‌ی شبه‌تصادفی داشته‌باشیم. در این صورت برای یک ثابت c و هر تابع $l : \mathbb{N} \to \mathbb{N}$ که در زمان چندجمله‌ای قابل محاسبه است، $BPTIME\left(S\big(l(n)\big)\right) \subseteq DTIME(2^{cl(n)})$.

اثبات. طبق تعریف زبان L را عضو $BPTIME\left(S\big(l(n)\big)\right)$ می‌دانیم اگر الگوریتم A روی ورودی $x \in \{0,1\}^n$ وجود داشته باشد که در زمان $cS(l(n))$ برای یک ثابت c اجرا شود و نابرابری زیر در حالتی که احتمال روی r تصادفی که توزیع یکنواخت روی $\{0,1\}^m$ در نظر گرفته‌شده صحیح باشد:

$$\Pr[A(x,r) = L(x)] \geq {}^2\!/_3$$

حال به ازای ورودی x برای تمام $z \in \{0,1\}^{l(n)}$، $A\big(x, G(z)\big)$ را محاسبه کرده و جواب اکثریت را به عنوان خروجی برمی‌گردانیم. اگر $\Pr[A(x,G(z)) = L(x)] < {}^2\!/_3 - 0.1$ در این صورت یک تمایزدهنده برای تولیدکننده‌ی شبه-

[1] در کتاب "روش‌های احتمالاتی" نوشته‌ی ج. اسپنسر و ن. الن می‌توانید مجموعه‌ی جالبی از این روش‌ها را در حوزه‌های مختلف مشاهده کنید. بعضی از این روش‌ها به قدری اعجاب‌انگیز هستند که باور اولیه مبنی بر اینکه تصادفی‌سازی قدرت ذاتی به راه‌حل مسائل اضافه می‌کند را توجیه می‌کند.

[2] Derandomization

[3] Pseudorandom Generator

[4] Time-Constructible

تصادفی داریم؛ با استفاده از تبدیل کوک-لوین می‌توانیم مداری بسازیم که x را با اتصال ثابت به آن داده ایم و تابع $A(x,r)$ را از روی r محاسبه می‌کند. اندازه‌ی این مدار از $O(S(l(n))^2)$ است که برای n به اندازه‌ی کافی بزرگ از $S(l(n))^3$ کمتر می‌باشد و این متناقض با تولیدکننده‌ی شبه‌تصادفی بودن است. پس فرضمان غلط است و داریم $\Pr[A(x,G(z)) = L(x)] \geq {}^2/_3 - 0.1$. درنتیجه از آن جا که می‌توانیم جواب صحیح را برای تعداد زیادی از ورودی‌ها به طور اتصال ثابت به الگوریتم بدهیم ثابت می‌شود که $L \in DTIME(2^{cl(n)})$. □

نتیجه 1. موارد زیر با توجه به لم فوق به راحتی قابل بررسی هستند:

1) اگر برای یک ثابت $0 < \epsilon$ یک $2^{\epsilon l}$- تولیدکننده‌ی شبه‌تصادفی وجود داشته باشد داریم $BPP = P$.
2) اگر برای یک ثابت $0 < \epsilon$ یک 2^{l^ϵ}- تولیدکننده‌ی شبه‌تصادفی وجود داشته باشد داریم $BPP \subseteq QuasiP$ که در آن $QuasiP = DTIME(2^{polylog(n)})$.
3) اگر برای هر ثابت $c > 0$ یک l^c- تولیدکننده‌ی شبه‌تصادفی وجود داشته باشد داریم $BPP \subseteq SUBEXP$ که در آن $SUBEXP = \bigcap_{\epsilon>0} DTIME(2^{n^\epsilon})$.

تعریف 3. سختی حالت میانگین[5] یک تابع $f: \{0,1\}^n \to \{0,1\}^n$ که آن را با $H_{avg}(f)$ نشان می‌دهیم بزرگترین عدد Sای است که برای هر مدار C روی n ورودی که اندازه‌ی آن حداکثر S باشد نابرابری زیر در حالتی که احتمال روی x تصادفی که توزیع یکنواخت روی $\{0,1\}^n$ در نظر گرفته‌شده صحیح باشد:

$$\Pr[C(x) = f(x)] < {}^1/_2 + {}^1/_S$$

همچنین سختی بدترین حالت را نیز به طور مشابه تعریف می‌کنیم به طوری که سمت راست نابرابری بالا 1 باشد و آن را برای تابع f با $H_{wrs}(f)$ نشان می‌دهیم.

قضیه 1. اگر $S: \mathbb{N} \to \mathbb{N}$ و $f \in DTIME(2^{O(n)})$ وجود داشته باشد به طوری که برای هر n داشته‌باشیم $H_{avg}(f)(n) \geq S(n)$، در این صورت برای یک ثابت $0 < \delta$، یک $S(\delta l)^\delta$- تولیدکننده‌ی شبه‌تصادفی داریم.

اثبات. این قضیه در [2] اثبات شده‌است. □

قضیه 2. اگر $S: \mathbb{N} \to \mathbb{N}$ و $f \in E = DTIME(2^{O(n)})$ وجود داشته باشد به طوری که برای هر n داشته‌باشیم $H_{wrs}(f)(n) \geq S(n)$، در این صورت برای یک ثابت $0 < \delta$، یک $S(\delta l)^\delta$- تولیدکننده‌ی شبه‌تصادفی داریم و نتایج زیر برقرارند:

1) اگر $f \in E$ و ثابت $0 < \epsilon$ وجود داشته باشد که $H_{wrs}(f)(n) \geq 2^{\epsilon n}$ داریم $BPP = P$.
2) اگر $f \in E$ و ثابت $0 < \epsilon$ وجود داشته باشد که $H_{wrs}(f)(n) \geq 2^{n^\epsilon}$ داریم $BPP \subseteq QuasiP$.
3) اگر $f \in E$ و ثابت $0 < \epsilon$ وجود داشته باشد که $H_{wrs}(f)(n) \geq n^{w(10)}$ داریم $BPP \subseteq SUBEXP$.

اثبات. این قضیه با استفاده از قضیه‌ی 1 و قضیه‌ی 19.27 از [1] قابل اثبات است. □

[5] Average-Case Hardness

3. ساختار تولیدکننده‌های شبه‌تصادفی

قضیه 3. (قضیه‌ی یا-أ[6]) فرض کنید Y یک توزیع روی $\{0,1\}^n$ باشد. اگر $S > 10n$ و $0 < \epsilon$ وجود داشته‌باشد به طوری که برای هر مدار C از اندازه‌ی حداکثر $2S$ نابرابری زیر به ازای احتمال روی r که از توزیع Y انتخاب شده برقرار باشد:

$$\Pr[C(r_1, \dots, r_{i-1}) = r_i] \leq {}^1/_2 + {}^\epsilon/_m$$

در این صورت Y یک (S, ϵ)- شبه‌تصادفی است.

لم 2. اگر $f \in E$ وجود داشته باشد که $H_{avg}(f)(n) \geq n^4$ آن‌گاه یک $(l+1)$- تولیدکننده‌ی شبه‌تصادفی G وجود دارد.

اثبات. G را به این صورت تعریف می‌کنیم که به ازای هر $z \in \{0,1\}^l$ داریم $G(z) = z \circ f(z)$. طول خروجی برابر $l + 1$ است و ما هم همین را می‌خواستیم. برای اثبات این‌که خروجی یک $((l+1)^3, {}^1/_{10})$- شبه‌تصادفی است از قضیه‌ی 3 استفاده می‌کنیم. یعنی کافی است نشان دهیم مدار C از سایز $l^4 > 2(l+1)^3$ و $i \in [l+1]$ وجود ندارد به طوری که:

$$\Pr[C(r_1, \dots, r_{i-1}) = r_i] > {}^1/_2 + {}^1/_{20(l+1)}$$

از آن‌جایی که برای هر $i \leq l$، i-امین بیت $G(z)$ توزیع یکنواخت دارد و مستقل از $i-1$ بیت اول است با هیچ مداری نمی‌تواند با احتمال بیشتر از ${}^1/_2$ حدس زده شود. برای $i = l+1$ نیز معادله‌ی فوق به صورت زیر در می‌آید:

$$\Pr[C(z) = f(z)] > {}^1/_2 + {}^1/_{20(l+1)} > {}^1/_2 + {}^1/_{l^4}$$

که نابرابری فوق متناقض با فرض $H_{avg}(f)(n) \geq n^4$ می‌باشد. □

با تعمیم این ایده می‌توان تولیدکننده‌های شبه‌تصادفی با طول دلخواه ساخت. در واقع در صورتی که بخواهیم طول خروجی تولیدکننده‌ی شبه‌تصادفی را k بیت افزایش دهیم کافی است ساختاری مشابه ساختار زیر تعریف کنیم:

$$G(z_1, \dots, z_l) = z^1 \circ f(z^1) \circ z^2 \circ f(z^2) \circ \dots \circ z^k \circ f(z^k)$$

که z^i نشان‌دهنده‌ی i-امین بلوک ${}^l/_k$ بیتی از z است.

4. قطعی‌سازی تحت فرضیاتی در پیچیدگی محاسبات

تعریف 4. فرض کنید $A \in F^{n \times n}$ ماتریسی روی میدان F باشد. دائم[7] A به صورت زیر تعریف می‌شود:

$$perm(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a(i, \sigma(i))$$

---

[6] Yao's Theorem
[7] Permanent

قضیه 4. فرض کنید $BPP \neq EXP$. در این صورت برای هر $L \in BPP$ یک الگوریتم قطعی A با زمان $2^{n^{o(1)}}$ وجود دارد به طوری که برای تعداد نامتناهی n رابطه‌ی زیر در حالتی که احتمال روی x با توزیع یکنواخت روی $\{0,1\}^n$ محاسبه شود برقرار است:

$$\Pr[A(x) = L(x)] \geq 1 - 1/n$$

اثبات. در این‌جا به بیان ایده‌ی کلی اثبات پرداخته و از جزئیات صرف نظر می‌کنیم. برای شروع می‌توانیم فرض کنیم $EXP \subseteq P_{/poly}$؛ چرا که در غیر این صورت مسائلی در EXP وجود دارند که مرتبه‌ی پیچیدگی مدارشان فوق چندجمله‌ای است و چنین مسائلی می‌توانند در ساخت تولیدکننده‌های شبه تصادفی قدرتمندی استفاده شوند که حکم را نتیجه دهند. درنتیجه $EXP \subseteq P_{/poly}$ و خواهیم داشت $EXP = PH$. در این صورت با استفاده از قضایای تودا[8] و ولیانت[9] (قضایای 17.14 و 17.11 درمرجع [1]) می‌توان نتیجه گرفت که تابع دائم $perm$، $EXP\_complete$ است. از طرفی طبق فرض قضیه $perm$ در BPP نیست. حال با استفاده از قضیه‌ی 1 و قضیه‌ی 19.27 از [1] باید یک تولیدکننده‌ی شبه‌تصادفی G بسازیم که از $perm$ به عنوان تابع سخت خودش استفاده کند. سپس با برهان خلف نشان می‌دهیم که نتیجه‌ی قضیه‌ی 1 صحیح است. در صورت برقراری فرض خلف یک دنباله از مدارهای با اندازه‌ی چند جمله‌ای تمایزدهنده وجود دارد و یک الگوریتم احتمالاتی با زمان چندجمله‌ای وجود دارد که می‌تواند با گرفتن طول ورودی مدار تمایزدهنده‌اش را با احتمال خطای حداکثر $1/n$ برگرداند که ما با یک فرض ساده‌سازی این احتمال را به $1/n^2$ کاهش می‌دهیم. با استفاده از این الگوریتم می‌توانیم یک الگوریتم T پیدا کنیم که تابع $perm$ را یاد بگیرد و با استفاده از T می‌توان به یک الگوریتم احتمالاتی چندجمله‌ای برای تابع دائم رسید که از هیچ دانای کلی استفاده نمی‌کند. در واقع برای این‌که مدار برای ورودی به طول n را تولید کنیم کافی‌است به طور استقرایی و با استفاده از ویژگی خودکاهشی سراشیبی[10] تابع $perm$ آن را از مدار برای ورودی به طول $n-1$ تولید کنیم و در نتیجه دانای کل برای T جهت تولید مدار برای ورودی به طول n را پیاده‌سازی کنیم. حال چون طبق فرض $BPP \neq EXP$ و بر اساس $EXP \subseteq P_{/poly}$ نتیجه گرفتیم که تابع دائم $perm$، $EXP\_complete$ است به تناقض می‌رسیم. □

تعریف 5. مجموعه‌ی مدارهای جبری که چندجمله‌ای های متحد با صفر را مصاحبه می‌کنند $ZEROP$ نامیده می‌شود.

تعریف 6. تابع f روی اعداد صحیح را عضو $AlgP_{/poly}$ گوییم اگر بتواند توسط یک مدار جبری با اندازه‌ی چندجمله‌ای و عملگرهای +، - و × محاسبه شود.

در ادامه به ارتباط کران پایین برای مدارها و قطعی‌سازی اشاره کرده و بیان چند لم بدون ذکر اثباتشان می‌پردازیم که در اثبات قضیه‌ی بعدی مورد استفاده قرار می‌گیرند.

لم 3. اگر $EXP \subseteq P_{/poly}$ آن‌گاه $EXP = MA$.

لم 4. اگر $ZEROP \in P$ و $perm \in AlgP_{/poly}$ آن‌گاه $P^{perm} \subseteq NP$.

لم 5. اگر $NEXP \subseteq P_{/poly}$ آن‌گاه $NEXP = EXP$.

[8] Toda's Theorem
[9] Valiant's Theorem
[10] Downward Self-Reducibility

قضیه 5. اگر $ZEROP \in P$، آن‌گاه یا $NEXP \not\subseteq P_{/poly}$ و یا $perm \notin AlgP_{/poly}$.

اثبات. حکم را با برهان خلف ثابت می‌کنیم. فرض کنید داریم:

$$ZEROP \in P \qquad (1)$$

$$NEXP \subseteq P_{/poly} \qquad (2)$$

$$perm \in AlgP_{/poly} \quad (3)$$

از (2) و لم 3 و 5 نتیجه می‌شود $NEXP = EXP = MA$. حال از آن‌جا که $MA \subseteq PH$ و با استفاده از قضیه‌ی تودا به دست می‌آید $PH \subseteq P^{\#P}$. از طرفی طبق قضیه‌ی ولیانت تابع $perm$، $\#P\_complete$ است. پس تحت فرضیات ما

$$NEXP \subseteq P^{perm}$$

حل از آن‌جا که فرض کردیم $ZEROP \in P$ از (3) و لم 4 نتیجه می‌شود $NEXP \subseteq NP$ که متناقض با قضیه‌ی سلسله‌مراتب زمانی غیر قطعی[11] است. پس (1) و (2) و (3) نمی‌توانند همزمان صحیح باشند و حکم برقرار است. □

5. منابع

[1] Arora, Sanjeev, and Boaz Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[2] C. Umans. Pseudo-random generators for all hardnesses. *J. Comput. Syst. Sci.*,67(2):419–440, 2003

[11] Nondeterministic Time Hierarchy Theorem