


دانشکده‌ی علوم ریاضی

مقدمه‌ای پیشرفته بر رمزنگاری ۲۵ مهر ۱۳۹۱

جلسه‌ی ۱۰: ویژگی‌های تمایزناپذیری محاسباتی

مدرس: شهرام خزائی *نگارنده: حمیدرضا خوش‌اخلاق*

۱ نمادگذاری

PPT: مجموعه الگوریتم‌های تصادفی چندجمله‌ای[۱]
nuPPT: مجموعه الگوریتم‌های تصادفی چندجمله‌ای غیریکنواخت[۲]
NEG: مجموعه توابع ناچیز[۳]
Poly: مجموعه توابع چندجمله‌ای

۲ یادآوری تعریف تمایزناپذیری محاسباتی

تعریف ۱ *فرض کنید $\{X_n\}_{n\in\mathbb{N}}$ و $\{Y_n\}_{n\in\mathbb{N}}$ گردایه[۴]هایی باشند به طوریکه $\{X_n\}$ و $\{Y_n\}$ توزیع‌هایی روی $\{0,1\}^{\ell(n)}$ هستند. می‌گوییم $\{X_n\}_{n\in\mathbb{N}}$ و $\{Y_n\}_{n\in\mathbb{N}}$ تمایزناپذیر محاسباتی هستند (و با نماد $\{X_n\}_{n\in\mathbb{N}} \approx \{Y_n\}_{n\in\mathbb{N}}$ نمایش می‌دهیم) اگر:*

$$\forall \mathcal{D} \in \mathsf{nuPPT}\ \exists \varepsilon(n) \in \mathsf{NEG} : |\Pr[t \leftarrow X_n : \mathcal{D}(t) = 1] - \Pr[t \leftarrow Y_n : \mathcal{D}(t) = 1]| < \varepsilon(n)$$

تعریف ۲ *می‌گوییم تمایزگر $\mathcal{D}$ توزیع‌های X و Y را با احتمال (امتیاز[۵]) ε تمایز می‌دهد اگر:*

$$|Pr[t \leftarrow X : \mathcal{D}(t) = 1] - \Pr[t \leftarrow Y : \mathcal{D}(t) = 1]| > \varepsilon$$

۳ ویژگی‌های تمایزناپذیری محاسباتی

۱.۳ ترایایی - لم هایبرید

لم ۱ *اگر $H^0, H^1, ..., H^m$ دنباله‌ای از توزیع‌ها باشند و یک تمایزگر $\mathcal{D}$ وجود داشته باشد که H^0 و H^m را با احتمال ε تمایز دهد، آنگاه وجود دارد $i \in [0, 1, ..., m-1]$ به طوریکه $\mathcal{D}$ توزیع‌های H^i و H^{i+1} را با احتمال*

[۱] probabilistic polynomial time
[۲] non-uniform
[۳] negligible
[۴] ensemble
[۵] advantage

$\frac{\varepsilon}{m}$ *تمایز می‌دهد.*

برهان. تعریف می‌کنیم:

$$g_i = \Pr\{t \longleftarrow H^i : \mathcal{D}(t) = ۱\}$$

چون $H^۰$ و H^m با احتمال ε تمایز داده می‌شوند، داریم: $|g_۰ - g_m| > \varepsilon$. حال با برهان خلف فرض می‌کنیم:

$$\forall i : |g_i - g_{i+۱}| \leq \frac{\varepsilon}{m}$$

در نتیجه داریم:

$$\begin{aligned} |g_0 - g_m| &= |g_0 - g_1 + g_1 - g_2 + g_2 - .... + g_{m-1} - g_m| \\ &= |\sum_{i=0}^{m-1}(g_i - g_{i+1})| \\ &\leq \sum_{i=0}^{m-1}|g_i - g_{i+1}| \\ &\leq m(\frac{\varepsilon}{m}) = \varepsilon \end{aligned}$$

که این نتیجه با فرض اولیه در تناقض است و در نتیجه حکم ثابت می‌شود. ■

نتیجه ۱ اگر $X \approx Y$ و $Y \approx Z$ آنگاه $X \approx Z$.

تعریف ۳ *گردایه‌ی $X = \{X_n\}$ قابل تولید به صورت کارا [۶] است اگر الگوریتم $S \in$ nuPPT وجود داشته باشد، به طوریکه متغیرهای تصادفی X_n و $S(۱^n)$ دارای توزیع یکسان باشند.*

فرض کنید توزیع‌های $\{X_n\}_{n\in\mathbb{N}}$ و $\{Y_n\}_{n\in\mathbb{N}}$ و $\{Z_n\}$ توزیع‌های قابل تولید به صورت کارا و دو به دو تمایزناپذیر باشند. می‌خواهیم ثابت کنیم که توزیع‌های $\{X_nY_n\}_{n\in\mathbb{N}}$ و $\{Z_n^۱Z_n^۲\}_{n\in\mathbb{N}}$ نیز تمایزناپذیر هستند. که $Z_n^۱$ و $Z_n^۲$ دارای توزیع یکسان Z_n و مستقل هستند. تعریف می‌کنیم:

$$\begin{aligned} H^۱ &= X_nY_n \\ H^۲ &= X_nZ_n \\ H^۳ &= Z_n^۱Z_n^۲ \end{aligned}$$

طبق نتیجه‌ای که از لم هایبرید گرفتیم، کافی است ثابت کنیم که $H^۲ \approx H^۱$ و $H^۲ \approx H^۳$.

۲.۳ حفظ تمایزناپذیری تحت عملیات کارا

قضیه ۲ *اگر $\{Y_n\}_{n\in\mathbb{N}} \approx \{X_n\}_{n\in\mathbb{N}}$ آنگاه به ازای هر $M \in$ nuPPT داریم: $\{M(Y_n)\}_{n\in\mathbb{N}} \approx \{M(X_n)\}_{n\in\mathbb{N}}$*

برهان.(برهان خلف) فرض می‌کنیم تمایزگر $\mathcal{D}$ برای توزیع‌های $M(X_n)$ و $M(Y_n)$ وجود داشته باشد. یعنی تابع ناچیز ε وجود دارد به طوریکه $\mathcal{D}$ توزیع‌های $M(X_n)$ و $M(Y_n)$ را با احتمال $\varepsilon(n)$ از هم تمایز می‌دهد:

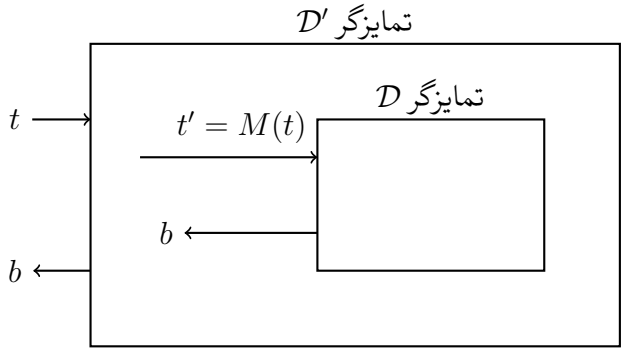
$$|\Pr[t \leftarrow M(X_n) : \mathcal{D}(t) = ۱] - \Pr[t \leftarrow M(Y_n) : \mathcal{D}(t) = ۱]| > \varepsilon(n)$$

حال می‌توان تمایزگر $\mathcal{D}'(\cdot) = \mathcal{D}(M(\cdot))$ را ساخت که $\{X_n\}$ و $\{Y_n\}$ را با احتمال $\varepsilon(n)$ از هم تمایز می‌دهد:

[۶] efficiently constructible

$$|\Pr[t \leftarrow X_n : \mathcal{D}(M(t)) = ۱] - \Pr[t \leftarrow Y_n : \mathcal{D}(M(t)) = ۱]| > \varepsilon(n)$$

و این با فرض اولیه که $\{X_n\}$ و $\{Y_n\}$ تمایزناپذیر هستند، تناقض دارد. ■



۳.۳ تمایزناپذیری تحت نمونه‌برداری چندجمله‌ای

تعریف ۴ *گردایه‌های $X = \{X_n\}$ و $Y = \{Y_n\}$ را تحت نمونه‌برداری چندجمله‌ای، تمایزناپذیر می‌گوییم هرگاه:*
$\forall \mathcal{D} \in \mathsf{nuPPT}, \forall m(\cdot) \in \mathsf{Poly}\ \exists\, \varepsilon \in \mathsf{NEG}$:
$|\Pr[(t^1, t^2, ..., t^{m(n)}) \leftarrow (X_n^1, X_n^2, ..., X_n^{m(n)}) : \mathcal{D}(t^1, t^2, ..., t^{m(n)}) = 1] -$
$\Pr[(t^1, t^2, ..., t^{m(n)}) \leftarrow (Y_n^1, Y_n^2, ..., Y_n^{m(n)}) : \mathcal{D}(t^1, t^2, ..., t^{m(n)}) = 1]| \leq \varepsilon(n)$
که X_n^iها دارای توزیع یکسان X_n و مستقل هستند.

قضیه ۳ *اگر گردایه‌های $X = \{X_n\}$ و $Y = \{Y_n\}$ تمایزناپذیر محاسباتی باشند، آنگاه تحت نمونه‌برداری چندجمله‌ای نیز تمایزناپذیر محاسباتی هستند.*

برهان.(برهان خلف) فرض میکنیم تمایزگر $\mathcal{D}$ و چندجمله‌ایهای $m(\cdot)$ و $p(\cdot)$ وجود دارند به طوریکه برای تعداد نامتناهی n داریم:

$$\Delta(n) \stackrel{def}{=} |\Pr[(t^1, t^2, ..., t^m) \leftarrow (X_n^1, X_n^2, ..., X_n^m) : \mathcal{D}(t^1, t^2, ..., t^m) = 1] -$$
$$\Pr[(t^1, t^2, ..., t^m) \leftarrow (Y_n^1, Y_n^2, ..., Y_n^m) : \mathcal{D}(t^1, t^2, ..., t^m) = 1]| > \frac{1}{p(n)}$$

$(m \stackrel{def}{=} m(n))$. حال تعریف می کنیم:

$$H_۰ = (X^۱, X^۲, ..., X^m)$$
$$H_۱ = (Y^۱, X^۲, ..., X^m)$$
$$\vdots$$
$$H_i = (Y^۱, ..., Y^i, X^{i+۱}, ..., X^m)$$
$$\vdots$$
$$H_m = (Y^۱, Y^۲, ..., Y^m)$$

طبق فرض خلف بالا $\mathcal{D}$ می‌تواند H_0 و H_m را با احتمال $\frac{1}{p(n)}$ تمایز دهد. در نتیجه طبق لم هایبرید iای وجود دارد به طوریکه $\mathcal{D}$ هایبریدهای H_i و H_{i+1} را با احتمال $\frac{1}{p(n)m(n)}$ تمایز می‌دهد. حال از روی $\mathcal{D}$ تمایزگر $\mathcal{D}'$ را می‌سازیم که می‌تواند توزیع‌های X و Y را تمایز دهد. با ورودی α (که دارای توزیع X_n یا Y_n است) الگوریتم $\mathcal{D}'$ چنین عمل می‌کند:

۱) یک مقدار تصادفی k از بازه $\{0, 1, ..., m-1\}$ انتخاب می‌کند.
۲) k نمونه مستقل از X_n تولید می‌کند: $x^1, ..., x^k$
۳) $m-k-1$ نمونه مستقل نیز از Y_n تولید می‌کند: $y^{k+2}, ..., y^m$
۴) مقدار $\mathcal{D}(x^1, ..., x^k, \alpha, y^{k+2}, ..., y^m)$ را به عنوان خروجی بیرون می‌دهد.

واضح است که الگوریتم $\mathcal{D}'$ می‌تواند در زمان چندجمله‌ای اجرا شود. همچنین داریم:

$$\Pr[t \leftarrow X_n : \mathcal{D}'(t) = 1] = \frac{1}{m} \sum_{k=0}^{m-1} \Pr[t \leftarrow H_n^{k+1} : \mathcal{D}(t) = 1]$$
$$\Pr[t \leftarrow Y_n : \mathcal{D}'(t) = 1] = \frac{1}{m} \sum_{k=0}^{m-1} \Pr[t \leftarrow H_n^{k} : \mathcal{D}(t) = 1]$$

درنتیجه:

$$|\Pr[t \leftarrow X_n : \mathcal{D}'(t) = 1] - \Pr[t \leftarrow Y_n : \mathcal{D}'(t) = 1]|$$
$$= \frac{1}{m} \cdot |\Pr[t \leftarrow H_n^m : \mathcal{D}(t) = 1] - \Pr[t \leftarrow H_n^0 : \mathcal{D}(t) = 1]| = \frac{\Delta(n)}{m} > \frac{1}{p(n)m(n)}$$

بنابراین الگوریتم $\mathcal{D}'$ می‌تواند X و Y را از هم تمایز دهد که این با فرض اولیه در تناقض است. ■