**مقدمه‌ای پیشرفته بر رمزنگاری** ۳۰ مهر ۱۳۹۱

# جلسه‌ی ۱۱ : تمایزناپذیری و شبه‌تصادفی

*مدرس: شهرام خزائی* *نگارنده: آرمن آبنوسی*

با توجه به تمایزناپذیری محاسباتی، توزیع‌های شبه‌تصادفی را تعریف می‌کنیم. یک توزیع را شبه‌تصادفی می‌گوییم اگر از توزیع یکنواخت تمایزناپذیر باشد.

## ۱ خانواده توزیع‌ها و تمایزناپذیری محاسباتی

**تعریف ۱** *(خانواده توزیع‌ها) یک دنباله از توزیع‌های احتمال $X_1, X_2, \ldots$ را یک خانواده از توزیع‌ها می‌گویند و با $\{X_n\}_{n\in\mathbb{N}}$ و یا به اختصار $\{X_n\}$ نشان می‌دهند.*

تمایزناپذیری خانواده‌ای از توزیع‌ها هم مانند تمایزناپذیری دو توزیع تعریف می‌شود که در زیر این تعریف را ارایه می‌کنیم:

**تعریف ۲** *(تمایزناپذیری دو خانواده از توزیع‌ها) دو خانواده از توزیع‌ها $X = \{X_n\}_{n\in\mathbb{N}}$ و $X = \{Y_n\}_{n\in\mathbb{N}}$ را تمایزناپذیر محاسباتی می‌نامیم و می‌نویسیم $X \approx Y$ ، اگر برای هر تمایزگر PPT یک تابع ناچیز نظیر $\epsilon(\cdot)$ وجود داشته باشد که:*

$$|\Pr[\mathcal{D}(X_n) = 1] - \Pr[\mathcal{D}(Y_n) = 1]| \leq \epsilon(n)$$

## ۲ ویژگی‌های تمایزناپذیری محاسباتی

دو ویژگی زیر را برای تمایزناپذیری داریم:

**ویژگی ۱** (بستار تحت عملیات کارا) اگر $\{Y_n\} \approx \{X_n\}$ آن گاه برای هر PPT نظیر $M$ داریم:

$$\{M(X_n)\} \approx \{M(Y_n)\}$$

**ویژگی ۲** (لم هایبرید) برای یک دنباله توزیع احتمال $X_1, X_2, \ldots, X_m$ اگر تمایزگر $\mathcal{D}$ وجود داشته باشد که با احتمال $\epsilon$، $X_1$ را از $X_m$ تمییز دهد، آن گاه وجود دارد $i$-ای که $\mathcal{D}$ با احتمال حداقل $\frac{\epsilon}{m}$، $X_i$ را از $X_{i+1}$ تمییز می‌دهد.

ویژگی سوم تمایزناپذیری لم پیش‌بینی[1] است. این لم بیان می‌کند که اگر یک مهاجم بتواند دو توزیع احتمال را از یکدیگر تمییز دهد، آن گاه این مهاجم همچنین می‌تواند برای هر نمونه تشخیص دهد که از کدام یک از توزیع‌ها تولید شده است. لم پیش‌بینی را با بیان رسمی در زیر ارایه می‌کنیم.

[1] prediction lemma

**لم ۱** *(لم پیش‌بینی) فرض کنید یک* PPT *مانند* $\mathcal{D}$ *تمایزگری برای خانواده های* $\{X_n^0\}$ *و* $\{X_n^1\}$ *باشد که در آن‌ها هر* $X_n^0$ *و* $X_n^1$ *یک توزیع بر روی* $\{0,1\}^{m(n)}$ *است (که* $m(\cdot)$ *یک چندجمله‌ای است)؛ اگر یک تمایزگر* $\mathcal{D}$ *که* PPT *است وجود داشته باشد که این دو خانواده را با احتمال* $\mu(n)$ *تمییز دهد، در این صورت یک الگوریتم* PPT *مانند* $\mathcal{A}$ *وجود دارد که:*

$$\Pr[b \leftarrow \{0,1\}, t \leftarrow X_n^b : \mathcal{A}(t) = b] \geq \frac{1}{2} + \frac{\mu(n)}{2}$$

**برهان.** بدون کاستن از کلیت مسأله فرض کنید که $\mathcal{D}$ با گرفتن نمونه‌ای تولید شده از $X_n^1$ با احتمال بیشتری مقدار یک را به عنوان خروجی بدهد. نشان می‌دهیم که $\mathcal{D}$ می‌تواند شرایط گفته شده در بالا برای $\mathcal{A}$ را داشته باشد و بنابراین $\mathcal{D}$ یک تمایزگر مطابق حکم لم می‌باشد:

$$\begin{aligned}
\Pr[b \leftarrow \{0,1\}; t \leftarrow X_n^b : \mathcal{D}(t) = b] &= \frac{1}{2}\Pr[t \leftarrow X_n^1 : \mathcal{D}(t) = 1] + \frac{1}{2}\Pr[t \leftarrow X_n^0 : \mathcal{D}(t) \neq 1] \\
&= \frac{1}{2}\Pr[t \leftarrow X_n^1 : \mathcal{D}(t) = 1] + \frac{1}{2}(1 - \Pr[t \leftarrow X_n^0 : \mathcal{D}(t) = 1]) \\
&= \frac{1}{2} + \frac{1}{2}\Pr[t \leftarrow X_n^1 : \mathcal{D}(t) = 1] - \frac{1}{2}\Pr[t \leftarrow X_n^0 : \mathcal{D}(t) = 1] \\
&= \frac{1}{2} + \frac{\mu(n)}{2}
\end{aligned}$$

■

# ۳ توزیع شبه‌تصادفی

با توجه به آنچه در ابتدا ذکر شد، با استفاده از تعریف تمایزناپذیری است که شبه‌تصادفی بودن معنا می‌گیرد. بنابراین در اینجا خانواده‌ای از توزیع‌های شبه‌تصادفی را به صورت رسمی به ترتیب زیر تعریف می‌کنیم:

**تعریف ۳** *(خانواده توزیع‌های شبه‌تصادفی) خانواده توزیع‌های* $\{X_n\}_n$ *را که در آن* $X_n$ *یک توزیع احتمال بر روی* $\{0,1\}^{l(n)}$ *برای یک چندجمله‌ای* $l(\cdot)$ *است را شبه‌تصادفی گویند اگر* $\{X_n\}_n \approx \{U_{l(n)}\}_n$

این تعریف بدان معناست که برای آنکه یک توزیع احتمال شبه‌تصادفی باشد، باید در تمام آزمایشات آماری رفتاری مانند رفتار توزیع یکنواخت داشته باشد.
آزمایشات آماری وجود دارند که اگر یک توزیع احتمال این آزمایشات را با موفقیت بگذراند می‌توان نشان داد که در سایر آزمایش‌ها هم موفق خواهد بود. (به چنین آزمایش‌هایی کامل می‌گویند.) یکی از این آزمایش‌ها، آزمایش بیت بعدی[۲] است که در زیر بیان می‌شود.

# ۴ آزمایش بیت بعدی

می‌گوییم که یک توزیع، آزمایش بیت بعدی را با موفقیت پشت سر می‌گذارد اگر هیچ مهاجم کارآمدی نتواند با داشتن یک پیشوند از رشته‌ای که توسط این توزیع تولید شده است بیت بعدی این رشته را با احتمال قابل توجهی بیش از ۱/۲ حدس بزند. به صورت رسمی تعریف زیر را داریم:

[۲] next bit test

**تعریف ۴** *می‌گویند خانواده $\{X_n\}_n$ که در آن $X_n$ یک توزیع احتمال بر روی $\{۰,۱\}^{l(n)}$ برای یک چندجمله‌ای $l(\cdot)$ است، در آزمایش بیت بعدی موفق است اگر برای هر مهاجم $\mathcal{A}$ یک تابع ناچیز نظیر $\epsilon(n)$ وجود داشته باشد، به طوری که $\forall n \in \mathbb{N}$ و $\forall i \in [۰,\dots,l(n)]$، داشته باشیم:*

$$\Pr[t \leftarrow X_n : \mathcal{A}(۱^n, t_۱ t_۲ \dots t_i) = t_{i+۱}] < \frac{۱}{۲} + \epsilon(n)$$

*که در آن منظور از $t_i$ بیت $i$ -ام از رشته $t$ است.*

قضیه زیر بیان می‌کند که آزمایش بیت بعدی کامل است.

**قضیه ۲** *اگر یک خانواده $\{X_n\}_n$ از احتمال‌ها آزمایش بیت بعدی را با موفقیت پشت سر بگذارد آن گاه $\{X_n\}_n$ شبه‌تصادفی است.*

**برهان.** فرض خلف کنید که یک تمایزگر PPT مانند $\mathcal{D}$، یک چندجمله‌ای مانند $p(\cdot)$ و نامتناهی $n \in \mathbb{N}$ وجود دارند که $\mathcal{D}$ می‌تواند $X_n$ و $U_{l(n)}$ را با احتمال $\frac{۱}{p(n)}$ برای هر چنین $n$-ای تمییز دهد. ماشین $\mathcal{A}$ را که برای هر چنین $n$-ای بیت بعدی $X_n$ را حدس می‌زند می‌سازیم.
یک دنباله از توزیع‌های هایبرید را طبق تعریف زیر در نظر بگیرید.

$$H_n^i = \{x \leftarrow X_n : u \leftarrow U_{l(n)} : x_۱ \dots x_i u_{i+۱} u_{i+۲} \dots u_{l(n)}\}$$

واضح است که $H_n^۰ = U_{l(n)}$ و $H_n^{l(n)} = X_n$. بنابراین $\mathcal{D}$ با احتمال $\frac{۱}{p(n)}$، $H_n^۰$ را از $H_n^{l(n)}$ تمییز می‌دهد. با توجه به لم هایبرید نتیجه می‌شود که یک $i \in [۰, l(n)]$ وجود دارد که $\mathcal{D}$ با احتمال $\frac{۱}{p(n)l(n)}$ می‌تواند $H_n^i$ و $H_n^{i+۱}$ را از یکدیگر تمییز دهد. ولی تنها اختلاف میان $H^i$ و $H^{i+۱}$ این است که در $H^{i+۱}$ بیت $(i+۱)$-ام برابر $x_{i+۱}$ است ولی در $H^i$ این بیت برابر $u_{i+۱}$ است. بنابراین $\mathcal{D}$ با داشتن پیشوند $x_۱ \dots x_i$ می‌تواند $x_{i+۱}$ را از بیتی که با توزیع یکنواخت مقداردهی شده است تمییز دهد. و این به آن معناست که $\mathcal{D}$ می‌تواند $x_{i+۱}$ را از $\overline{x}_{i+۱}$ تمییز دهد.
به صورت دقیق‌تر توزیع زیر را در نظر بگیرید:

$$\overline{H}_n^i = \{x \leftarrow X_n : u \leftarrow U_{l(n)} : x_۱ \dots x_{i-۱} \overline{x}_i u_{i+۱} u_{i+۲} \dots u_{l(m)}\}$$

مشاهده می‌شود که اگر با احتمال نیم از $H_n^{i+۱}$ و با احتمال نیم از $\overline{H}_n^{i+۱}$ نمونه برداریم معادل این است که از $H_n^i$ نمونه برداشته‌ایم. اگر این تساوی را در قسمت دوم عبارت زیر قرار دهیم:

$$\left| \Pr[t \leftarrow H_n^{i+۱} : \mathcal{D}(t) = ۱] - \Pr[t \leftarrow H_n^i : \mathcal{D}(t) = ۱] \right|$$

نتیجه می‌شود که:

$$\left| \Pr[t \leftarrow H_n^{i+۱} : \mathcal{D}(t) = ۱] - (\tfrac{۱}{۲} \Pr[t \leftarrow H_n^{i+۱} : \mathcal{D}(t) = ۱] + \tfrac{۱}{۲} \Pr[t \leftarrow \overline{H}_n^{i+۱} : \mathcal{D}(t) = ۱] \right|$$

و با ساده کردن این عبارت نتیجه زیر حاصل می‌شود:

$$\tfrac{۱}{۲} \left| \Pr[t \leftarrow H_n^{i+۱} : \mathcal{D}(t) = ۱] - \Pr[t \leftarrow \overline{H}_n^{i+۱} : \mathcal{D}(t) = ۱] \right|$$

با ترکیب این نتیجه با آنچه که در بالا گفته شد مبنی بر اینکه $\mathcal{D}$ با احتمال $\frac{1}{p(n)l(n)}$ می‌تواند $H_n^i$ و $H_n^{i+1}$ را از یکدیگر تمییز دهد نتیجه می‌شود که $\mathcal{D}$ با احتمال $\frac{2}{p(n)l(n)}$ می‌تواند $H_n^{i+1}$ و $\overline{H}_n^{i+1}$ را از یکدیگر تمییز دهد. با استفاده از لم پیش‌بینی می‌توان گفت که باید یک ماشین $\mathcal{A}$ وجود داشته باشد که:

$$\Pr[b \leftarrow \{0,1\}; t \leftarrow H_n^{i+1,b} : \mathcal{D}(t) = b] > \frac{1}{2} + \frac{1}{p(n)l(n)}$$

که در آن $H_n^{i+1,1}$ معرف $H_n^{i+1}$ و $H_n^{i+1,0}$ معرف $\overline{H}_n^{i+1}$ است؛ یعنی $\mathcal{A}$ می‌تواند تشخیص دهد که یک نمونه از $H_n^{i+1}$ تولید شده است و یا $\overline{H}_n^{i+1}$. در این صورت می‌توان از $\mathcal{A}$ برای ساخت ماشین $\mathcal{A}'$ استفاده کرد که $\mathcal{A}'$ می‌تواند $x_{i+1}$، یعنی بیت $(i+1)$-ام را در یک رشته شبه‌تصادفی حدس بزند. ولی با ساخت $\mathcal{A}'$ شبه‌تصادفی بودن رشته نقض می‌شود. در نتیجه فرض خلف باطل است. کافی است نشان دهیم $\mathcal{A}'$ چگونه کار می‌کند. الگوریتم زیر را برای $\mathcal{A}'$ در نظر بگیرید:

---

**الگوریتم ۱** الگوریتم برای ماشین $\mathcal{A}'$

---

**ورودی:** $t_1 t_2 \dots t_i$

**خروجی:** حدس $\hat{t}_{i+1}$ برای $t_{i+1}$

۱. تعداد $l(n) - i$ بیت تصادفی را بردار $(u_{i+1} \dots u_{l(n)} \leftarrow U^{l(n)-i})$.

۲. ماشین $\mathcal{A}$ را با ورودی $t_1 \dots t_i u_{i+1} \dots u_{l(n)}$ اجرا کن و خروجی آن را برابر $b$ قرار بده.

۳. اگر $b = 1$ آنگاه مقدار $\hat{t}_{i+1} = u_{i+1}$ را به عنوان خروجی ارایه کن. در غیر این صورت مقدار $\hat{t}_{i+1} = 1 - u_{i+1}$ را به عنوان خروجی ارایه کن.

---

با این الگوریتم خواهیم داشت:

$$\begin{aligned}\Pr[t \leftarrow X_n : \mathcal{A}'(1^n, t_1 \dots t_i) &= t_{i+1}] = \Pr[b \leftarrow \{0,1\}; t \leftarrow H_n^{i+1,b} : \mathcal{A}(t) = 1] \\ &> \frac{1}{2} + \frac{1}{p(n)l(n)}\end{aligned}$$

همان طور که گفته شد این بدان معناست که $\mathcal{A}'$ می‌تواند بیت‌های یک رشته شبه‌تصادفی را با احتمال غیرقابل چشم‌پوشی حدس بزند که این نقض تعریف شبه‌تصادفی بودن است. بنابراین فرض خلف باطل است و قضیه اثبات شده است.

■

# ۵ مولدهای شبه‌تصادفی

**تعریف ۵** *(مولدهای شبه‌تصادفی) فرض کنید $l(\cdot)$ یک چندجمله‌ای و $G$ یک الگوریتم معین چندجمله‌ای باشد که برای هر ورودی $s$، الگوریتم $G$ یک رشته به طول $l(|s|)$ را به عنوان خروجی می‌دهد. $G$ را مولد شبه‌تصادفی می‌گوییم اگر دو شرط زیر برقرار شوند:*

۱. *(گسترش) به ازای هر $n$ داشته باشیم: $l(n) > n$*

۲. (*شبه‌تصادفی بودن*) *خانواده* $\{G(u_n)\}_{n\in\mathbb{N}}$ *شبه‌تصادفی باشد.*

بنا بر این تعریف، می‌توان گفت که شبه‌تصادفی بودن حالت خاصی از تمایزناپذیر بودن است.
یک روش ابتدایی برای ساخت مولد شبه‌تصادفی که ممکن است به ذهن خطور کند استفاده از جایگشت یک طرفه‌ای نظیر $f$ است؛ به این ترتیب که ابتدا یک seed مانند $s$ به تابع $f$ می‌دهیم، خروجی آن را $(f(s))$ دریافت می‌کنیم و سپس $f(\cdot)$ را بر روی $f(s)$ اجرا می‌کنیم و این عملیات را تکرار می‌کنیم. خروجی نهایی از الصاق خروجی های هر مرحله به یکدیگر به طوری که $s$ در سمت راست‌ترین بیت‌ها (کم ارزش‌ترین بیت‌ها) و $f^n(s)$ در سمت چپ‌ترین بیت‌ها قرار گیرند به دست می‌آید. یعنی $G(s) = f^n(s)||f^{n-1}(s)||\dots||f(s)||s$.
در این روش از این خاصیت استفاده کرده‌ایم که اگر پیشوندی از $G(s)$ داده شود، بدست آوردن ادامه آن معادل با پیدا کردن معکوس تابع $f$ است و این با توجه به یک‌طرفه بودن $f$ ممکن نیست.
با وجود اینکه نمی‌توانیم تمام رشته $G(s)$ را با داشتن یک پیشوند از آن با احتمالی مناسب حدس بزنیم ولی این به معنای عدم توانایی در حدس زدن بیت‌ها نیست. زیرا تعریف تابع یک‌طرفه به گونه‌ای است که به ما این امکان را می‌دهد که مثلاً تابع یک طرفه‌ای داشته باشیم که چند بیت ابتدای ورودی را به عنوان پیشوندی از خروجی تکرار کند؛ در این صورت می‌توانیم تعدادی از بیت‌ها را به یقین بدانیم. با تغییر این روش به طوری که از بیت‌های هاردکور[۳] استفاده کند می‌توان روشی به دست آورد که بیت‌های غیرقابل پیش‌بینی به وجود آورد.
ولی اینکه چرا در این روش از جایگشت یک‌طرفه و نه از تابع یک‌طرفه استفاده کردیم می‌تواند به دو دلیل باشد. اولاً با توجه به روش مذکور مشخص می‌شود که نیاز داریم که دامنه و برد $f$ برابر باشند (زیرا در هر مرحله، خروجی مرحله قبل را به عنوان ورودی استفاده می‌کنیم). دوماً با توجه به شرط شبه‌تصادفی بودن برای مولد و نیز اینکه خروجی یک مرحله ورودی مرحله بعد است، می‌خواهیم که اگر ورودی $(x)$ از توزیعی یکنواخت (یا تقریباً یکنواخت) باشد، خروجی $f(x)$ هم دارای توزیعی یکنواخت (یا تقریباً یکنواخت) باشد، زیرا در این صورت مقداری که در هر مرحله بدست می‌آید تصادفی (یا شبه‌تصادفی) خواهد بود. این در حالی است که توابع یک‌طرفه‌ای که جایگشت نیستند دارای این خاصیت نمی‌باشند؛ یعنی خروجی می‌تواند توزیعی متفاوت از توزیع ورودی داشته باشد.

[۳] hard core