رمزنگاری، کوییز دوم

سعید هدایتیان (ش.د.۹۷۱۰۰۲۹۲)

۲۱ اسفند ۱۳۹۸

سؤال ۱.

۱.۱) برای اثبات اینکه $\Delta(X,Y)$ یک متریک است چهار شرط را چک می کنیم.

$$\Delta(X,Y) \geqslant 0 \tag{۱}$$

چون $\Delta(X,Y)$ حاصل جمع تعدادی قدرمطلق است.

$$\Delta(X,Y) = 0 \Leftrightarrow X = Y \tag{۲}$$

به وضوح اگر $X = Y$ ، آنگاه $\Delta(X,Y) = 0.$ برعکس این موضوع هم درست است. چون از ۰ بودن فاصله آماری دو توزیع می توان نتیجه گرفت که همه قدر مطلق ها صفر هستند یعنی

$$\forall \omega \in \Omega : Pr[X = \omega] = Pr[Y = \omega].$$

پس دو توزیع عیناً مثل همدیگر هستند.

$$\Delta(X,Y) = \Delta(Y,X) \tag{۳}$$

چون $|Pr[X = \omega] - Pr[Y = \omega]| = |Pr[Y = \omega] - Pr[X = \omega]|$ به سادگی این خاصیت هم نتیجه می شود.

$$\Delta(X,Y) \leqslant \Delta(X,Z) + \Delta(Y,Z) \tag{۴}$$

طبق نامساوی مثلثی می توان دید که

$$\forall \omega \in \Omega : |Pr[X = \omega] - Pr[Y = \omega]| \leqslant |Pr[X = \omega] - Pr[Z = \omega]| + |Pr[Z = \omega] - Pr[Y = \omega]|.$$

با جمع کردن این نامساوی ها به ازای همه ω ها رابطه چهارم هم نتیجه می شود. پس فاصله آماری دو توزیع در واقع یک متریک است.

۲.۱) مجموعه Ω را می توان به سه مجموعه A و B و C افراز کرد به گونه ای که

$$\forall a \in A : Pr[X = a] > Pr[Y = a]$$

و

$$\forall b \in B : Pr[X = b] < Pr[Y = b]$$

و

$$\forall c \in C : Pr[X = c] = Pr[Y = c]$$

.

با توجه به افراز های داده شده می توان دید که بیشترین مقدار برای $|Pr[X \in S] - Pr[Y \in S]|$ زمانی رخ می دهد که $S = A$ یا $S = B$.
همچنین می توان نوشت

$$\sum_{a\in A} Pr[X = a] - Pr[Y = a] - \sum_{b\in B} Pr[Y = b] - Pr[X = b] + \sum_{c\in C} Pr[X = c] - Pr[Y = c]$$
$$= \sum_{\omega\in\Omega} Pr[X = \omega] - \sum_{\omega\in\Omega} Pr[Y = \omega] = 1 - 1 = 0.$$

چون $\sum_{c\in C} Pr[X = c] - Pr[Y = c] = 0$ پس می توان نتیجه گرفت

$$\sum_{a\in A} Pr[X = a] - Pr[Y = a] = \sum_{b\in B} Pr[Y = b] - Pr[X = b].$$

اما دقت کنید که فاصله آماری X و Y هم در واقع نصف حاصل جمع همین دو مجموع بالا است. یعنی

$$\Delta(X, Y) = \frac{1}{2}(\sum_{a\in A} Pr[X = a] - Pr[Y = a] + \sum_{b\in B} Pr[Y = b] - Pr[X = b]).$$

پس فاصله آماری دو تابع را می توان به صورت

$$\sum_{a\in A} Pr[X = a] - Pr[Y = a]$$

یا

$$\sum_{b\in B} Pr[Y = b] - Pr[X = b]$$

هم نوشت.

۳.۱) ابتدا دقت کنید که چنانچه تمایزگر D به صورت زیر تعریف شود مزیت آن برابر فاصله آماری X_0 و X_1 خواهد بود.

$$D(\omega) = \begin{cases} 1 & Pr(X_1 = \omega) > Pr(X_0 = \omega) \\ 0 & o.w. \end{cases}$$

حال اثبات می کنیم مزیت از این مقدار بیشتر نمی شود. از برهان خلف استفاده می کنیم. داریم

$$|Pr[\omega \leftarrow X_0 : D_{OPT}(\omega) = 1] - Pr[\omega \leftarrow X_1 : D_{OPT}(\omega) = 1]|$$
$$> \Delta(X_0, X_1) \implies |\sum_{\omega \in \Omega} \frac{1}{2} Pr(D_{OPT}(\omega) = 1)(Pr(X_0 = \omega) - Pr(X_1) = \omega)|$$
$$> \Delta(X_0, X_1) \implies \frac{1}{2} \sum_{\omega \in \Omega} A - |A| > 0.$$

($A = Pr(X_0 = \omega) - Pr(X_1) = \omega$) که به وضوح نادرست است.

سؤال ۲.

خیر هیچ یک مولد شبه تصادفی امنی نیستند. دو تمایزگر زیر را در نظر بگیرید.

$$D_1(s_1||s_2) = \begin{cases} 1 & s_1 = \overline{s_2} \\ 0 & o.w. \end{cases}$$

و

$$D_2(s_1||s_2) = \begin{cases} 1 & s_2 = 0^{|s|} \\ 0 & o.w. \end{cases}$$

این دو تمایزگر می توانند مولد را با مزیت غیر ناچیزی برای توابع گفته شده تشخیص دهند. مزیت هر دو به شیوه زیر محاسبه می شود.

$$Pr[x \leftarrow U_n; y = g(x) : D(y) = 1] = 1$$
$$Pr[x \leftarrow U_{2n} : D(x) = 1] = 2^{-n}$$

پس مزیت برابر $1 - 2^{-n}$ است.

سؤال ۳.

می دانیم $|g(U_n)| = 2^n$. مجموعه $\{0,1\}^{n+1}$ را به دو زیرمجموعه با تعداد اعضای برابر $A = g(U_n)$ و

$A - \{0,1\}^{n+1} = B$ افراز کنید. حال فرض کنید تمایزگر D به ازای همه A ها خروجی ۱ و به ازای همه B ها خروجی ۰ بدهد. مزیت این تمایزگر غیر ناچیز خواهد بود.

$$Pr(x \leftarrow U_n; y = g(x) : D(y) = 1) = 1$$

و

$$Pr(x \leftarrow U_{n+1}; D(x) = 1) = \frac{1}{2}$$

پس مزیت برابر $\frac{1}{2}$ است.

سؤال ۴.

۱.۴) در حالتی که تمایزگر کارا باشد، مثلا می توان دید که مضارب ۴ امکان ندارد حاصلضرب دو عدد n بیتی اول باشند. پس مثلا می توان به ازای همه مضارب ۴ خروجی را ۰ (یعنی تمایزگر بگوید از U_{2n} انتخاب شده)و در غیر اینصورت ۱ داد. در این حالت مزیت برابر است با

$$Pr(p, q \leftarrow U_n; x = pq : D(x) = 1) = 1,$$

$$Pr(x \leftarrow U_{2n}; D(x) = 1) = \frac{3}{4}$$

$$\implies \mu = \frac{1}{4}$$

۲.۴) این دو متغییر هم قابل تمایز هستند. می توان دید که کم ارزش ترین بیت Y همیشه ۰ است. با توجه به این موضوع تمایزگر D را در نظر بگیرید که اگر بیت کم ارزش ورودیش ۰ بود خروجی را ۱ کند(یعنی تمایزگر بگوید از توزیع Y آمده) و در غیر اینصورت خروجی ۰ بدهد. مزیت در این حالت برابر است با

$$Pr[a, b \leftarrow U_n; x = (a+b) \oplus a \oplus b : D(x) = 1] = 1,$$

$$Pr[x \leftarrow U_n : D(x) = 1] = \frac{1}{2}$$

$$\implies \mu = \frac{1}{2}.$$

۳.۴) با استفاده از کامپیوتر مقدار فاصله آماری دو متغییر تصادفی را برای n های ۲ تا ۱۰ محاسبه کردیم. با توجه به نتایج الگوی بدست آمده احتمالا رابطه زیر برای فاصله آماری X و Y برحسب n برقرار است:

$$\Delta_n(X, Y) = 2^{-\lfloor \frac{n}{2} \rfloor - 1}$$

و به نظر می رسد این دو توزیع تمایزپذیر نیستند.