Error clase Miércoles 22 de Marzo 2017

Fernando Krell

1. Problema Original

Demostrar que si G' es un generador pseudo-aleatorio, entonces la función $G(x) = G'(x)||G'(x+1)$ *NO* es necesariamente un generador psuedo-aleatorio.

Idea de la demostración: Construir PRG G' tal que $G'(x) = G'(x+1)$ cuando x es par *sin perder la pseudo-aleatoriedad de* G'.

2. Error

Sea $G'' : \{0,1\}^\lambda \to \{0,1\}^n$ un generador pseudo-aleatorio (PRG). Para obtener la propiedad deseada, en clases se propuso definir la función $G' : \{0,1\}^\lambda \to \{0,1\}^n$ como $G''(x+1)$ si x es par y $G''(x)$ si x es impar. De esta forma, $G'(x) = G'(x+1)$ cuando x es par y por lo tanto la función original G no es PRG (distinguidor sólo necesita verificar que la primera mitad es igual a la segunda mitad).

Sin embargo, la función G' definida en el párrafo anterior *NO es necesariamante psuedo-aleatoria*. Imaginemos un tercer generador pseudo-aleatorio

$$G^* : \{0,1\}^{\lambda-1} \to \{0,1\}^n, \text{ tal que } G''(x_{1\ldots\lambda}) := G^*(x_{1\ldots\lambda-1})||x_\lambda$$

.

Claramente G'' es PRG, pues los primeros bits son generados por G^* y el último bit x_λ es independiente de los primeros. (Recordar que en la definición the PRGs el input x es elegido uniformemete, y por lo tanto x_λ es un bit uniforme en tal caso).

Ahora bien, calculemos el valor de $G'(x)$.

Caso x es par:

$$G'(x) = G''(x+1) = G^*(x_{1\ldots\lambda})||1$$

Caso x es impar:

$$G'(x) = G''(x) = G^*(x_{1\ldots\lambda})||1$$

Por lo tanto, el último bit generado por G' es *siempre* 1, y concluímos que G' no es PRG.

3. Solución Correcta

Sea $G'' : \{0,1\}^{\lambda-1} \to \{0,1\}^n$ una PRG y definamos

$$G' : \{0,1\}^{\lambda} \to \{0,1\}^n \text{ tal que } G'(x_{1\ldots\lambda}) := G''(x_{1\ldots\lambda-1})$$

Mostramos ahora que este último G' *sí* es psuedo-aleatorio. Sea D' un distinguidor para G' tal que

$$|\Pr[D'(G'(x)) = 1]| - \Pr[D'(u) = 1]| \geq 1/p(n)$$

.

Construímos un distinguidor (reducción) D'' para G'' de la siguiente manera: con entrada z, ejecutamos $D'(z)$ para obtener un bit b. Luego retornamos b.

Análisis:

Caso z es uniforme en $\{0,1\}^n$:

$$\Pr[D''(u) = 1] \;=\; \Pr[D'(u) = 1]$$

Caso z es $G''(x)$, para x uniforme en $\{0,1\}^{\lambda-1}$:

$$\begin{aligned}
\Pr_{x\sim U_{\lambda-1}}[D''(G''(x)) = 1] &= \Pr_{x\sim U_{\lambda-1}}[D'(G''(x)) = 1] \\
&= \Pr_{x\sim U_{\lambda}}[D'(G''(x_{1\ldots\lambda-1})) = 1] \texttt{ \# agregamos un bit dummy} \\
&= \Pr_{x\sim U_{\lambda}}[D'(G'(x)) = 1]
\end{aligned}$$

Por lo tanto,

$$|\Pr[D''(G''(x)) = 1]| - \Pr[D''(u) = 1] = |\Pr[D'(G'(x)) = 1] - \Pr[D'(u) = 1]| \geq 1/p(n)$$

Dado que asumimos que G'' es PRG, podemos deducir que tal D' no existe, y concluímos finalmente que G' sí es PRG.