MA-53G Intr. a la Criptografía **Semestre Primavera, 1996**

Cátedra No. 17 : 22 de Octubre

Transcriptor: Julio Aracena L.

Ya se han definido las funciones de un sentido débil y las funciones de un sentido fuerte. Claramente, es más conveniente tener una función de un sentido débil que una función de un sentido fuerte. Pero, si tenemos una función de sentido débil podemos construir una función de sentido fuerte, como lo muestra el siguiente teorema.

Teorema 1 *Existen funciones de un sentido débil si y sólo si existen funciones de un sentido fuerte*

Dem: La implicancia hacia la izquierda es evidente a partir de las definiciones. La demostración de la implicancia en el otro sentido la haremos por contradicción. Sea $f : \{0,1\}^* \to \{0,1\}^*$, función de un sentido débil, luego existe un polinomio $q(\cdot)$, tal que para todo adversario A existe un $n_0 \in I\!N$ tal que $\forall n \geq n_0$

$$Pr_{x\in\{0,1\}^*}[A \text{ tiene éxito en } f] \leq 1 - \tfrac{1}{q(n)}$$

(entenderemos por A tiene éxito en f el evento $\{x : A(f(x)) \in f^{-1}(f(x))\}$)

De ahora en adelante, las probabilidades durante la demostración son calculadas uniformemente sobre todos los valores posibles del string $x \in \{0,1\}^n$ y sobre las fuentes de aleatoriedad de los algoritmos probabilísticos.

Fijemos el polinomio $q(\cdot)$, que sin pérdida de generalidad podemos considerar creciente, y definamos la función: $g : \{0,1\}^* \to \{0,1\}^*$, tal que si $x \in \{0,1\}^m$, y $x = x_1x_2\cdots x_Nu$, con $N = 2nq(n)$, donde n es tal que:

$$2n^2q(n) \leq m < 2(n+1)^2q(n+1)$$

, entonces $g(x) = g(x_1x_2\ldots x_Nu) = f(x_1)\circ f(x_2)\circ\cdots\circ f(x_N), \quad x_i \in \{0,1\}^n$. Luego, la imagen de x por g corresponde a una cadena de largo Nn.

Afirmación: g es una función de un sentido fuerte.

Dem: (Afirmación) Supongamos que g no es de un sentido fuerte, i.e. que existe un adversario A' y un polinomio $q'(\cdot)$, tal que para una infinidad de m's :
$Pr[A'$ tenga éxito en $g] \geq \frac{1}{q'(m)}$. (A' tiene éxito en g significa que si la salida de A' es $z_1 z_2 \cdots z_N$, entonces $f(z_i) = f(x_i), \forall i \leq N$). Fijemos m y consideremos el siguiente algoritmo A que, como veremos, invierte f con una probabilidad que contradice el hecho de que f es función de un sentido débil. Este algoritmo recibe como entrada $y = f(x)$, y usa un valor arbitrario fijo u de largo $m - Nn$.

1. Para $i = 1, \ldots, N$ hacer
2. Repetir $2nNq'(m)$ veces
3. Elejir $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_N \in \{0,1\}^n$ al azar.
4. Calcular $g(x_1 \cdots x_{i-1} x x_{i+1} \cdots x_N u) = f(x_1) \cdots f(x_{i-1}) f(x) f(x_{i+1}) \cdots f(x_N)$ sea $z = A'(g(x_1 x_2 \cdots x_{i-1} x x_{i+1} \cdots x_N u))$.
5. Si A' tiene éxito, entonces $z = z_1 z_2 \cdots z_i \cdots z_N$, donde $f(z_j) = f(x_j)$, $\forall j \neq i$ y $f(z_i) = f(x) = y$, entonces entregamos como salida z_i, en caso contrario, continuamos con la próxima iteración.

Queremos demostrar que $Pr[A$ tenga éxito en $f]$ sea mayor o igual a $1 - \frac{1}{q(n)}$.
Para ello demostraremos que existe un indice $i \in \{1, \ldots N\}$ y un $x \in \{0,1\}^n$, tal que

$$Pr[A'(x_1 x_2 \ldots x_{i-1} x x_{i+1} \ldots x_N) \text{ tenga éxito }] \geq \frac{1}{2Nq'(m)}$$

Con este objeto, definamos a continuación, para cada $i = 1, \ldots, N$, y para todo $x \in \{0,1\}^n$:
$\varphi_{i,n}(x) = P[A'$ tiene éxito en $g(x_1 x_2 \ldots x_{i-1} x x_{i+1} \ldots x_N)]$, y
$E_n = \{x \in \{0,1\}^n : \forall i = 1, \ldots, N, \varphi_{i,n}(x) < \frac{1}{2Nq'(m)}\}$.
(*i.e.*, E_n representa el conjunto de los puntos en los cuales A tendrá una baja probabilidad de tener éxito). Supongamos por el momento que $|E_n| < \frac{2^n}{2q(n)}$. Luego

$$\begin{aligned} Pr[A(f(x)) \notin f^{-1}(f(x))] = {} & Pr[A(f(x)) \notin f^{-1}(f(x)) | x \in E_n] Pr[x \in E_n] \\ & + Pr[A(f(x)) \notin f^{-1}(f(x)) | x \notin E_n] Pr[x \notin E_n] \end{aligned}$$

Pero, $Pr[x \in E_n] = \frac{|E_n|}{|x \in \{0,1\}^n|} = \frac{1}{2q(n)}$, y sea a tal que $a \notin E_n$, luego existe un $i_0 \in \{1, \ldots, N\}$, tal que $\varphi_{i_0,n}(a) \geq \frac{1}{2Nq'(m)}$, por lo tanto

$$Pr[A'(x_1x_2 \ldots x_{i_0-1}ax_{i_0+1} \ldots x_N) \text{ no tenga éxito}] \leq (1 - \tfrac{1}{2Nq'(m)}), \text{ luego}$$
$$Pr[A \text{ no tenga éxito } |x \in E_n] \leq (1 - \tfrac{1}{2Nq'(m)})^{2Nq'(m)n},$$

pues son $2nNq'(m)$ iteraciones del algoritmo A' con entrada $g(x_1x_2 \ldots x_{i_0-1}ax_{i_0+1} \ldots x_Nu)$. Por consiguiente

$$Pr[A(f(x)) \notin f^{-1}(f(x))] \leq 1 \cdot \tfrac{1}{2q(n)} + (1 - \tfrac{1}{2Nq'(n)})^{2Nq'(n)n} \cdot 1 \leq \tfrac{1}{2q(n)} + e^{-n} < \tfrac{1}{q(n)}$$

donde $(1 - \frac{1}{2Nq'(n)})^{2Nq'(n)n} \leq e^{-n}$ para n suficientemente grande. Por lo tanto, $Pr[A \text{ tenga éxito}] > 1 - \frac{1}{q(n)}$. Pero, esto contradice el hecho que f es una función de un sentido débil, pues el mismo resultado lo podemos tener para una infinidad de n's, así g es una función de un sentido fuerte. □

Nosotros ahora sólo necesitamos demostrar que $|E_n| < \frac{2^n}{2q(n)}$. Supongamos que no se tiene, entonces

$\frac{1}{q'(m)} \leq Pr[A' \text{ tenga éxito en } g] = Pr[A' \text{ tenga éxito en } g \text{ y } \exists x_i; \varphi_{i,n}(x_i) < \frac{1}{2Nq'(m)}] +$
$Pr[A' \text{ tenga éxito en } g \text{ y } \forall x_i; \varphi_{i,n}(x_i) \geq \frac{1}{2Nq'(m)}]$
$\leq \sum_{i=1}^{N} Pr[A' \text{ tenga éxito en } g \text{ y } \varphi_{i,n}(x_i) < \frac{1}{2Nq'(m)}] + Pr[\forall x_i,\ \varphi_{i,n}(x_i) \geq \frac{1}{2Nq'(m)}]$
$\leq N\frac{1}{2Nq'(m)} + (Pr[x_i \notin E_n])^N \leq \frac{1}{2q'(m)} + (1 - \frac{1}{2q(n)})^N = \frac{1}{2q'(m)} + (1 - \frac{1}{2q(n)})^{2nq(n)} \leq \frac{1}{2q'(m)} + e^{-n} < \frac{1}{q'(m)}$, para n suficientemente grande.

Esto es una contradicción, luego $|E_n| < \frac{2^n}{2q(n)}$. □

Hay dos problemas asociados con la construcción de la función g en la demostración.

i) El tamaño de la entrada de g depende del valor de $q(\cdot)$, el cual puede que ser no conocido.

ii) El tamaño de la entrada de g depende de la función f. En la demostración, $m = O(n^2q(n))$.

Existen, sin embargo, construcciones más eficientes de una función de un sentido fuerte a partir de una función de un sentido débil.

1 Colección de funciones de un sentido

En muchas ocasiones se tiene un conjunto de funciones, mas bien que una sola, luego es necesario tener un concepto de colección de funciones de un sentido.

Definición 1 *Sea I un conjunto de índices , y $\forall i \in I$, sean D_i, R_i, conjuntos finitos. Una colección de funciones de un sentido es un conjunto $F = \{f_i : D_i \to R_i\}_{i \in I}$, satisfaciendo las siguientes condiciones:*

1) *Existe una máquina de Turing probabilista S_1, que en la entrada: 1^k encuentra $i \in \{0,1\}^k \cap I$.*

2) *Existe una máquina de Turing probabilista S_2, que con entrada $i \in I$ arroja como salida $x \in D_i$.*

3) *Existe una máquina de Turing probabilista A', tal que $\forall i \in I, \forall x \in D_i, A'(i,x) = f_i(x)$.*

4) *Para toda máquina de Turing probabilista A, para todo polinomio $q(\cdot)$, $\exists n_0 \in \mathbb{N}, \forall n \geq n_0$ tal que*

$$Pr[A(i, f_i(x)) \in f_i^{-1}(f_i(x))] \leq \frac{1}{q(n)},$$

donde la probabilidad es tomada sobre los i elegidos por S_1, los x elegidos por S_2 y la fuente de aleatoriedad de A.