El problema de la captura. Cuando consideramos cuantificadores aparece una dificultad. Por ejemplo, supongamos que queremos aplicar una sustitución δ a la frase $\exists x \,.\, x > y$, que es intuitivamente válida ya que no importa el valor de y, siempre existe un entero mayor x. Una aplicación "ingenua" de la sustitución, me daría $\exists x \,.\, x > e$ donde $e = \delta\ y$. En efecto, la variable x no se toca porque está ligada. Pero ¿qué pasa si e es x?, quedaría $\exists x \,.\, x > x$ que es falsa. Lo mismo ocurre, por ejemplo, si $e = x + 1$, quedaría $\exists x \,.\, x > x + 1$ que también es falsa.

Otro problema que puede observarse, es que como $\exists x \,.\, x > y$ por un lado, y $\exists z \,.\, z > y$ por otro sólo se diferencian en el nombre de la variable ligada, sustituir en uno u otro me debería dar resultados equivalentes. Pero, nuevamente para el caso en que $\delta\ y = x + 1$, en un caso obtenemos $\exists x \,.\, x > x + 1$, y en el otro $\exists z \,.\, z > x + 1$. No son equivalentes (la primera es falsa y la segunda es válida).

El problema es que al sustituir δ en $\exists x \,.\, x > y$, se está **capturando** la ocurrencia de x que era libre en $x + 1$, ahora pasa a ser ligada. Eso no debería ocurrir. Una solución es renombrar la variable ligada obteniendo por ejemplo $\exists z \,.\, z > y$ y luego sustituir, obteniendo $\exists z \,.\, z > x + 1$.

Otra posibilidad es hacer las dos cosas simultáneamente. Si bien es más complicado, es lógico hacerlo así ya que estamos definiendo justamente la sustitución, no deberíamos asumir que sabemos renombrar, ya que renombrar es sustituir un nombre por otro (en realidad esto es discutible, ya que el renombre es una forma un poco más sencilla de sustitución).

Conclusión: al aplicar una sustitución a una expresión de la forma $\forall v \,.\, b$ o $\exists v \,.\, b$, se propaga la sustitución y simultáneamente se renombra la variable v:

$$(\forall v \,.\, b)/\delta = \forall u \,.\, (b/[\delta|v : u])$$

donde u es una variable *nueva* y $[\delta|v : u]$ ya se definió: sustituye parecido a δ, salvo que a la variable v la reemplaza por u. Si no elegimos cuidadosamente a u, el problema de la captura persiste. Volviendo al ejemplo anterior, si en $\exists x \,.\, x > y$ aplicamos δ, donde $\delta\ y = x + z$, si sustituimos sin renombrar queda $\exists x \,.\, x > x + z$ que captura la x. Si renombramos x por z, nos queda $\exists z \,.\, z > x + z$ que captura la z. Para evitar la captura hay que elegir bien la variable nueva u: la variable u no debe ser **capturable**. ¿Y cuáles son las variables capturables? Son las que pueden aparecer por culpa de δ al aplicar la sustitución en b. Recordemos que δ sólo debe sustituir las variables libres de $\forall v \,.\, b$. O sea que las capturables son las que introduce δ para cada variable libre de $\forall v \,.\, b$. O sea, para todo $w \in FV(\forall v \,.\, b)$ debemos tener $u \notin FV(\delta\ w)$, o dicho de otro modo

$$u \notin \bigcup_{w \in FV(\forall v \,.\, b)} FV(\delta\ w)$$

o equivalentemente

$$u \notin \bigcup_{w \in FV(b)-\{v\}} FV(\delta\ w)$$

Para finalizar, entonces, agregamos las ecuaciones

$$\begin{array}{rcll} (\forall v\ .\ b)/\delta & = & \forall u\ .\ (b/[\delta|v:u]) & \text{donde } u \notin \bigcup_{w\in FV(b)-\{v\}} FV(\delta\ w) \\ (\exists v\ .\ b)/\delta & = & \exists u\ .\ (b/[\delta|v:u]) & \text{donde } u \notin \bigcup_{w\in FV(b)-\{v\}} FV(\delta\ w) \end{array}$$

Esto resuelve el problema, pero no está completamente definido ya que puede haber más de una variable u que satisfaga la condición (de hecho hay siempre una cantidad infinita de variables que la satisfacen). Debe determinarse un criterio para elegir la variable u: si v mismo satisface la condición, entonces $u = v$. En caso contrario, se elige u como la primera variable que la satisface en un orden preestablecido entre las variables.

Abreviatura. Hace algunos ejemplos, definimos id como la sustitución identidad, mapea cada variable v en la expresión v. Siendo cuidadosos, no deberíamos llamarla id ni identidad ya que mapea variables en términos.

Escribiremos $v_0 \to e_0, \ldots, v_{n-1} \to e_{n-1}$ para abreviar $[id|v_0 : e_0|\ldots|v_{n-1} : e_{n-1}]$.

Propiedades de la sustitución. Sean p una frase (entera o booleana), id la sustitución identidad, $\delta, \delta' \in \Delta$, las siguientes afirmaciones valen:

1. $p/id = p$.
2. Si δ y δ' coinciden en las variables libres de p, entonces da lo mismo aplicar δ o δ' a p. En símbolos:
$$(\forall w \in FV(p)\ .\ \delta\ w = \delta'\ w) \Longrightarrow p/\delta = p/\delta'$$
3. $FV(p/\delta) = \bigcup_{w\in FV(p)} FV(\delta\ w)$

Propiedades de la función $[\![\ ]\!]$.

Teorema de Coincidencia (TC). Si dos estados σ y σ' coinciden en las variables libres de p, entonces da lo mismo evaluar p en σ o σ'. En símbolos:

$$(\forall w \in FV(p)\ .\ \sigma\ w = \sigma'\ w) \Longrightarrow [\![p]\!]\sigma = [\![p]\!]\sigma'.$$

En particular, TC implica que el valor de un término cerrado es el mismo en cualquier estado, es decir, no depende del estado.

Teorema de Sustitución (TS). Si aplico la sustitución δ a p y luego evalúo en el estado σ, puedo obtener el mismo resultado a partir de p sin sustituir si evalúo en un estado que hace el trabajo de δ y de σ (en las variables libres de p). En símbolos:

$$(\forall w \in FV(p)\ .\ [\![\delta\ w]\!]\sigma = \sigma'\ w) \Longrightarrow [\![p/\delta]\!]\sigma = [\![p]\!]\sigma'.$$

Teorema de Sustitución Finita (TSF, corolario de TS).

$$[\![p/v_0 \to e_0, \ldots, v_{n-1} \to e_{n-1}]\!]\sigma = [\![p]\!][\sigma|v_0 : [\![e_0]\!]\sigma|\ldots|v_{n-1} : [\![e_{n-1}]\!]\sigma]$$

Teorema de Renombre (TR, corolario de TS y TC). Los nombres de la variables ligadas no tienen importancia. En símbolos,

$$u \notin FV(q) - \{v\} \Rightarrow [\![\forall u \;.\; q/v \to u]\!] = [\![\forall v \;.\; q]\!]$$

Demostraciones. Primero demostraremos que TSF y TR son corolarios de TS y TC:

Demostración de TSF. Sean la sustitución $\delta = v_0 \to e_0, ..., v_{n-1} \to e_n$ y el estado $\sigma' = [\sigma|v_0 : [\![e_0]\!]\sigma| \dots |v_{n-1} : [\![e_{n-1}]\!]\sigma]$.

TS dice que para demostrar TSF alcanza con comprobar que $\forall w \in FV(p) \;.\; [\![\delta \; w]\!]\sigma = \sigma' \; w$. Demostremos eso entonces. Sea $w \in FV(p)$. Si $w \in \{v_0, \dots, v_{n-1}\}$ (ojo! puede haber repeticiones), sea i el máximo tal que $w = v_i$. Tenemos $[\![\delta \; w]\!]\sigma = [\![\delta \; v_i]\!]\sigma = [\![e_i]\!]\sigma = \sigma' \; v_i = \sigma' \; w$. Si, por el contrario, $w \notin \{v_0, \dots, v_{n-1}\}$, también obtenemos $[\![\delta \; w]\!]\sigma = [\![id \; w]\!]\sigma = [\![w]\!]\sigma = \sigma \; w = \sigma' \; w$.

Demostración de TR. Sea $u \notin FV(q) - \{v\}$. Veamos que $[\![\forall u \;.\; (q/v \to u)]\!] = [\![\forall u \;.\; q]\!]$. Para ello, sea $\sigma \in \Sigma$:

$$\begin{array}{rcll}
[\![\forall u \;.\; (q/v \to u)]\!]\sigma & = & \forall n \in \mathbb{Z}.\; [\![q/v \to u]\!][\sigma|u : n] & \text{definición de } [\![\;]\!] \\
& = & \forall n \in \mathbb{Z}.\; [\![q]\!][\sigma|u : n|v : [\![u]\!][\sigma|u : n]] & \text{TSF} \\
& = & \forall n \in \mathbb{Z}.\; [\![q]\!][\sigma|u : n|v : n] & \text{definición de } [\![\;]\!] \\
& = & \forall n \in \mathbb{Z}.\; [\![q]\!][\sigma|v : n] & \text{TC } \wedge (u \notin FV(q) - \{v\}) \\
& = & [\![\forall v \;.\; q]\!]\sigma & \text{definición de } [\![\;]\!]
\end{array}$$

Demostración de TS. Sea

$$\Phi(p, \delta, \sigma, \sigma') = (\forall w \in FV(p).\; [\![\delta \; w]\!]\sigma = \sigma' \; w) \Rightarrow [\![p/\delta]\!]\sigma = [\![p]\!]\sigma'$$

demostraremos que para todo $p, \delta, \sigma, \sigma'$, $\Phi(p, \delta, \sigma, \sigma')$ se cumple, por inducción en p.

Si $p = 0$, se cumple ya que

$$\begin{array}{rcll}
[\![p/\delta]\!]\sigma & = & [\![0/\delta]\!]\sigma & p = 0 \\
& = & [\![0]\!]\sigma & \text{definición de substituir} \\
& = & 0 & \text{definición de } [\![\;]\!] \\
& = & [\![0]\!]\sigma' & \text{definición de } [\![\;]\!] \\
& = & [\![p]\!]\sigma' & p = 0
\end{array}$$

Lo mismo para las demás constantes numéricas y booleanas.

Si $p = v$, asumimos $\forall w \in FV(p).\; [\![\delta \; w]\!]\sigma = \sigma' \; w$, que equivale a $[\![\delta \; v]\!]\sigma = \sigma' \; v$. Luego, tenemos

$$\begin{array}{rcll}
[\![p/\delta]\!]\sigma & = & [\![v/\delta]\!]\sigma & p = v \\
& = & [\![\delta \; v]\!]\sigma & \text{definición de substituir} \\
& = & \sigma' \; v & \text{hipótesis} \\
& = & [\![v]\!]\sigma' & \text{definición de } [\![\;]\!] \\
& = & [\![p]\!]\sigma' & p = v
\end{array}$$

Si $p = e_0 + e_1$, asumimos $\forall w \in FV(p).\ [\![\delta\ w]\!]\sigma = \sigma'\ w$, que implica para $i \in \{0,1\}$, que $\forall w \in FV(e_i).\ [\![\delta\ w]\!]\sigma = \sigma'\ w$ y por hipótesis inductiva $\Phi(e_i, \delta, \sigma, \sigma')$ y $[\![e_i/\delta]\!]\sigma = [\![e_i]\!]\sigma'$. Entonces,

$$\begin{array}{rcll} [\![p/\delta]\!]\sigma & = & [\![(e_0+e_1)/\delta]\!]\sigma & p = e_0 + e_1 \\ & = & [\![(e_0/\delta)+(e_1/\delta)]\!]\sigma & \text{definición de substituir} \\ & = & [\![e_0/\delta]\!]\sigma + [\![e_1/\delta]\!]\sigma & \text{definición de } [\![\ ]\!] \\ & = & [\![e_0]\!]\sigma' + [\![e_1]\!]\sigma' & \text{hipótesis inductiva} \\ & = & [\![e_0+e_1]\!]\sigma' & \text{definición de } [\![\ ]\!] \\ & = & [\![p]\!]\sigma' & p = e_0 + e_1 \end{array}$$

Lo mismo para los demás operadores unarios y binarios.

Si $p = \forall v\ .\ b$, asumimos $\forall w \in FV(p).\ [\![\delta\ w]\!]\sigma = \sigma'\ w$, que equivale a asumir que $\forall w \in FV(b) - \{v\}.\ [\![\delta\ w]\!]\sigma = \sigma'\ w$. Sean $u \notin \bigcup_{w \in FV(b)-\{v\}} FV(\delta\ w)$ y $n \in \mathbb{Z}$ arbitrarios. Sean $\delta_0 = [\delta|v : u]$, $\sigma_0 = [\sigma|u : n]$ y $\sigma'_0 = [\sigma'|v : n]$. Se puede demostrar que se cumple $\forall w \in FV(b).\ [\![\delta_0\ w]\!]\sigma_0 = \sigma'_0\ w$. En efecto, si $w = v$, entonces

$$\begin{array}{rcll} [\![\delta_0\ w]\!]\sigma_0 & = & [\![\delta_0\ v]\!]\sigma_0 & w = v \\ & = & [\![u]\!]\sigma_0 & \text{definición de } \delta_0 \\ & = & \sigma_0\ u & \text{definición de } [\![\ ]\!] \\ & = & n & \text{definición de } \sigma_0 \\ & = & \sigma'_0\ v & \text{definición de } \sigma'_0 \\ & = & \sigma'_0\ w & w = v \end{array}$$

En caso contrario, $w \neq v$ entonces

$$\begin{array}{rcll} [\![\delta_0\ w]\!]\sigma_0 & = & [\![\delta\ w]\!]\sigma_0 & \text{definición de } \delta_0 \text{ y } w \neq v \\ & = & [\![\delta\ w]\!]\sigma & \text{TC, definición de } \sigma_0 \text{ y } u \notin FV(\delta\ w) \\ & = & \sigma'\ w & \text{hipótesis y } w \neq v \\ & = & \sigma'_0\ w & \text{definición de } \sigma'_0 \text{ y } w \neq v \end{array}$$

Esto prueba $\forall w \in FV(b).\ [\![\delta_0\ w]\!]\sigma_0 = \sigma'_0\ w$. Por hipótesis inductiva, $[\![b/\delta_0]\!]\sigma_0 = [\![b]\!]\sigma'_0$. Luego,

$$\begin{array}{rcll} [\![p/\delta]\!]\sigma & = & [\![(\forall v\ .\ b)/\delta]\!]\sigma & p = \forall v\ .\ b \\ & = & [\![\forall u\ .\ (b/\delta_0)]\!]\sigma & \text{definición de sustituir} \\ & = & \forall n \in \mathbb{Z}.\ [\![b/\delta_0]\!]\sigma_0 & \text{definición de } [\![\ ]\!] \\ & = & \forall n \in \mathbb{Z}.\ [\![b]\!]\sigma'_0 & \text{hipótesis inductiva} \\ & = & [\![\forall v\ .\ b]\!]\sigma' & \text{definición de } [\![\ ]\!] \\ & = & [\![p]\!]\sigma' & p = \forall v\ .\ b \end{array}$$

que es lo queríamos comprobar.

Demostración de TC. TC se utiliza en TS, por lo tanto debe demostrarse sin utilizar TS, ni TSF ni TR. Se propone $\Phi(p, \sigma, \sigma') = (\forall w \in FV(p).\ \sigma\ w = \sigma'\ w) \Rightarrow [\![p]\!]\sigma = [\![p]\!]\sigma'$ y debe demostrarse que para todo p, σ, σ', $\Phi(p, \sigma, \sigma')$ vale por inducción en p. La prueba, más sencilla que la de TS, queda como ejercicio.