System Specification

December 1, 2020

This document is created directly from the definitions in the file `dqtt.ott`, with minor modifications listed below.

It is intended to specify, in a readable form, the syntactic type soundness proof.

Note: there is one change here from the syntax shown in the paper. We replace the pattern matching elimination form for Σ types with a slightly more general, but less familiar, form.

The reason for this change is that the Ott and LNgen tools limit language specifications to single binding only. This prevents us from the usual definition of the pattern matching elimination form for Σ-types. Instead, we use an elimination form called "spread" of the form

$$\textbf{spread}\, a \,\textbf{to}\, x \,\textbf{in}\, b$$

This syntactic form binds the variable x (corresponding to the first component of the product) in the body b. The body b must itself be a function, where the argument is the second component of the tuple.

In other words, we can encode an elimination of an argument a of type $\Sigma x{:}^{q}A.B$, that uses the usual pattern matching syntax

$$\textbf{let}\,(x, y) \;=\; a \;\textbf{in}\; b$$

by using the term

$$\textbf{spread}\, a \,\textbf{to}\, x \,\textbf{in}\, \lambda y :^{q} A.b$$

1 Grammar

$\mathit{usage},\ q,\ r,\ s$	$::=$		
$\mathit{tm},\ a,\ b,\ A,\ B,\ v,\ w$	$::=$		terms and types
	$\mid$	$\mathbf{Unit}$	
	$\mid$	$\mathbf{unit}$	
	$\mid$	$\mathbf{let}\,\mathbf{unit}\ =\ a\ \mathbf{in}\ b$	
	$\mid$	$\Pi x :^{q} A.B$	
	$\mid$	$\lambda x :^{q} A.a$	
	$\mid$	$a\ b$	
	$\mid$	$\Box_{q} A$	
	$\mid$	$\mathbf{let}\,\mathbf{box}\,x\ =\ a\ \mathbf{in}\ b$	
	$\mid$	$\mathbf{type}$	
	$\mid$	x	
	$\mid$	$\mathbf{box}_{q}\ a$	
	$\mid$	$\mathbf{let}\,x = a\ \mathsf{in}\ b$	
	$\mid$	$A_1 \oplus A_2$	
	$\mid$	$\mathbf{inj}_1\ a$	
	$\mid$	$\mathbf{inj}_2\ a$	
	$\mid$	$\mathbf{case}_{q}\ a\ \mathbf{of}\ b_1; b_2$	
	$\mid$	$\Sigma x{:}^{q} A.B$	
	$\mid$	(a, b)	
	$\mid$	$\mathbf{spread}\ a\ \mathbf{to}\ x\ \mathbf{in}\ b$	
	$\mid$	$(x : A)\&B$	
	$\mid$	$\&(a, b)$	
	$\mid$	$\mathbf{prj}_1\ a$	
	$\mid$	$\mathbf{prj}_2\ a$	
$\mathit{context},\ \Gamma$	$::=$		contexts
	$\mid$	$\varnothing$	
	$\mid$	$x{:}^{q} A$	
	$\mid$	$x{:}^{q} aA$	
Δ	$::=$		contexts
	$\mid$	$\varnothing$	
	$\mid$	$x{:}A$	
	$\mid$	$x{:}aA$	

2 Step relation

$\boxed{a \leadsto a'}$ *(small-step)*

$$\dfrac{a \leadsto a'}{a\ b \leadsto a'\ b}\ \textsc{S-AppCong} \qquad \dfrac{}{(\lambda x :^{q} A . a)\ b \leadsto a\{b/x\}}\ \textsc{S-Beta}$$

$$\dfrac{a \leadsto a'}{\mathbf{let\,unit}\ =\ a\ \mathbf{in}\ b \leadsto \mathbf{let\,unit}\ =\ a'\ \mathbf{in}\ b}\ \textsc{S-UnitCong} \qquad \dfrac{}{\mathbf{let\,unit}\ =\ \mathbf{unit}\ \mathbf{in}\ b \leadsto b}\ \textsc{S-UnitBeta}$$

$$\dfrac{a \leadsto a'}{\mathbf{let\,box}\,x\ =\ a\ \mathbf{in}\ b \leadsto \mathbf{let\,box}\,x\ =\ a'\ \mathbf{in}\ b}\ \textsc{S-BoxCong}$$

$$\dfrac{}{\mathbf{let\,box}\,x\ =\ \mathbf{box}_q\ a\ \mathbf{in}\ b \leadsto b\{a/x\}}\ \textsc{S-BoxBeta} \qquad \dfrac{a \leadsto a'}{\mathbf{case}_q\ a\ \mathbf{of}\ b_1; b_2 \leadsto \mathbf{case}_q\ a'\ \mathbf{of}\ b_1; b_2}\ \textsc{S-CaseCong}$$

$$\dfrac{}{\mathbf{case}_q\ (\mathbf{inj}_1\ a)\ \mathbf{of}\ b_1; b_2 \leadsto b_1\ a}\ \textsc{S-Case1Beta} \qquad \dfrac{}{\mathbf{case}_q\ (\mathbf{inj}_2\ a)\ \mathbf{of}\ b_1; b_2 \leadsto b_2\ a}\ \textsc{S-Case2Beta}$$

$$\dfrac{a \leadsto a'}{\mathbf{spread}\ a\ \mathbf{to}\ x\ \mathbf{in}\ b \leadsto \mathbf{spread}\ a'\ \mathbf{to}\ x\ \mathbf{in}\ b}\ \textsc{S-SpreadCong}$$

$$\dfrac{}{\mathbf{spread}\ (a_0, a_1)\ \mathbf{to}\ x\ \mathbf{in}\ b \leadsto b\{a_0/x\}\ a_1}\ \textsc{S-SpreadBeta} \qquad \dfrac{}{\mathbf{prj}_1\ \&(a, b) \leadsto a}\ \textsc{S-Prj1Beta}$$

$$\dfrac{}{\mathbf{prj}_2\ \&(a, b) \leadsto b}\ \textsc{S-Prj2Beta} \qquad \dfrac{a \leadsto a'}{\mathbf{prj}_1\ a \leadsto \mathbf{prj}_1\ a'}\ \textsc{S-Prj1Cong} \qquad \dfrac{a \leadsto a'}{\mathbf{prj}_2\ a \leadsto \mathbf{prj}_2\ a'}\ \textsc{S-Prj2Cong}$$

3 Typing relation

Another issue with Σ types is that Ott cannot express the complete typing rule for **spread**. Therefore we need to modify the generate Coq definition to include the appropriate substitution. This document includes the corresponding change in the typeset rule T-Spread.

$\boxed{\Delta;\Gamma \vdash a : A}$ *(Typing)*

T-sub

$$\frac{\begin{array}{c}\Delta;\Gamma_1 \vdash a : A\\ \Delta;\Gamma_1 \leq \Gamma_2\end{array}}{\Delta;\Gamma_2 \vdash a : A}$$

T-type

$$\frac{}{\varnothing;\varnothing \vdash \textbf{type} : \textbf{type}}$$

T-var

$$\frac{\begin{array}{c}x \notin \mathsf{dom}\,\Delta\\ \Delta;\Gamma \vdash A : \textbf{type}\end{array}}{\Delta, x{:}A; 0{\cdot}\Gamma, x{:}^{1}A \vdash x : A}$$

T-weak

$$\frac{\begin{array}{c}x \notin \mathsf{dom}\,\Delta\\ \Delta;\Gamma_1 \vdash a : B\\ \Delta;\Gamma_2 \vdash A : \textbf{type}\end{array}}{\Delta, x{:}A;\Gamma_1, x{:}^{0}A \vdash a : B}$$

T-def

$$\frac{\begin{array}{c}x \notin \mathsf{dom}\,\Delta\\ \Delta;\Gamma \vdash a : A\end{array}}{\Delta, x{:}aA; 0{\cdot}\Gamma, x{:}^{1}aA \vdash x : A}$$

T-weak-def

$$\frac{\begin{array}{c}x \notin \mathsf{dom}\,\Delta\\ \Delta;\Gamma_1 \vdash b : B\\ \Delta;\Gamma_2 \vdash a : A\end{array}}{\Delta, x{:}aA;\Gamma_1, x{:}^{0}aA \vdash b : B}$$

T-pi

$$\frac{\begin{array}{c}\Delta;\Gamma_1 \vdash A : \textbf{type}\\ \Delta, x{:}A;\Gamma_2, x{:}^{r}A \vdash B : \textbf{type}\end{array}}{\Delta;\Gamma_1 + \Gamma_2 \vdash \Pi x{:}^{q}A.B : \textbf{type}}$$

T-lam

$$\frac{\begin{array}{c}\Delta, x{:}A;\Gamma_1, x{:}^{q}A \vdash a : B\\ \Delta;\Gamma_2 \vdash A : \textbf{type}\end{array}}{\Delta;\Gamma_1 \vdash \lambda x{:}^{q}A.a : \Pi x{:}^{q}A.B}$$

T-app

$$\frac{\begin{array}{c}\Delta;\Gamma_1 \vdash a : \Pi x{:}^{q}A.B\\ \Delta;\Gamma_2 \vdash b : A\end{array}}{\Delta;\Gamma_1 + q{\cdot}\Gamma_2 \vdash a\, b : B\{b/x\}}$$

T-conv

$$\frac{\begin{array}{c}\Delta;\Gamma_1 \vdash a : A\\ \Delta;\Gamma_2 \vdash B : \textbf{type}\\ \Delta\{A\} \equiv \Delta\{B\}\end{array}}{\Delta;\Gamma_1 \vdash a : B}$$

T-unit

$$\frac{}{\varnothing;\varnothing \vdash \textbf{unit} : \textbf{Unit}}$$

T-Unit

$$\frac{}{\varnothing;\varnothing \vdash \textbf{Unit} : \textbf{type}}$$

T-UnitE

$$\frac{\begin{array}{c}\Delta;\Gamma_1 \vdash a : \textbf{Unit}\\ B_1 = B\{\textbf{unit}/y\}\\ \Delta;\Gamma_2 \vdash b : B_1\\ \Delta, y{:}\textbf{Unit};\Gamma_3, y{:}^{r}\textbf{Unit} \vdash B : \textbf{type}\end{array}}{\Delta;\Gamma_1 + \Gamma_2 \vdash \textbf{let}\,\textbf{unit}\ =\ a\ \textbf{in}\ b : B\{a/y\}}$$

T-Box

$$\frac{\Delta;\Gamma \vdash A : \textbf{type}}{\Delta;\Gamma \vdash \Box_q A : \textbf{type}}$$

T-box

$$\frac{\Delta;\Gamma \vdash a : A}{\Delta; q{\cdot}\Gamma \vdash \textbf{box}_q\, a : \Box_q A}$$

T-letbox

$$\frac{\begin{array}{c}\Delta;\Gamma_1 \vdash a : \Box_q A\\ \Delta, x{:}A;\Gamma_2, x{:}^{q}A \vdash b : B\{\textbf{box}_q\, x/y\}\\ \Delta, y{:}\Box_q A;\Gamma_3, y{:}^{r}\Box_q A \vdash B : \textbf{type}\end{array}}{\Delta;\Gamma_1 + \Gamma_2 \vdash \textbf{let}\,\textbf{box}\, x\ =\ a\ \textbf{in}\ b : B\{a/y\}}$$

T-sum

$$\frac{\begin{array}{c}\Delta;\Gamma_1 \vdash A_1 : \textbf{type}\\ \Delta;\Gamma_2 \vdash A_2 : \textbf{type}\end{array}}{\Delta;\Gamma_1 + \Gamma_2 \vdash A_1 \oplus A_2 : \textbf{type}}$$

T-inj1

$$\frac{\begin{array}{c}\Delta;\Gamma \vdash a : A_1\\ \Delta;\Gamma_1 \vdash A_2 : \textbf{type}\end{array}}{\Delta;\Gamma \vdash \textbf{inj}_1\, a : A_1 \oplus A_2}$$

T-inj2

$$\frac{\begin{array}{c}\Delta; \Gamma \vdash a : A_2 \\ \Delta; \Gamma_1 \vdash A_1 : \mathbf{type}\end{array}}{\Delta; \Gamma \vdash \mathbf{inj}_2\, a : A_1 \oplus A_2}$$

T-case

$$\frac{\begin{array}{c}1 \leq q \\ \Delta; \Gamma_1 \vdash a : A_1 \oplus A_2 \\ B_1 = B\{\mathbf{inj}_1\, x/y\} \\ B_2 = B\{\mathbf{inj}_2\, x/y\} \\ \Delta; \Gamma_2 \vdash b_1 : \Pi x :^q A_1.B_1 \\ \Delta; \Gamma_2 \vdash b_2 : \Pi x :^q A_2.B_2 \\ \Delta, y{:}A_1 \oplus A_2; \Gamma_3, y{:}^r A_1 \oplus A_2 \vdash B : \mathbf{type}\end{array}}{\Delta;\, q \cdot \Gamma_1 + \Gamma_2 \vdash \mathbf{case}_q\, a\, \mathbf{of}\, b_1; b_2 : B\{a/y\}}$$

T-Sigma

$$\frac{\begin{array}{c}\Delta; \Gamma_1 \vdash A : \mathbf{type} \\ \Delta, x{:}A; \Gamma_2, x{:}^r A \vdash B : \mathbf{type}\end{array}}{\Delta; \Gamma_1 + \Gamma_2 \vdash \Sigma x{:}^q A.B : \mathbf{type}}$$

T-Tensor

$$\frac{\begin{array}{c}\Delta; \Gamma_1 \vdash a : A \\ \Delta; \Gamma_2 \vdash b : B\{a/x\} \\ \Delta, x{:}A; \Gamma_3, x{:}^r A \vdash B : \mathbf{type}\end{array}}{\Delta;\, q \cdot \Gamma_1 + \Gamma_2 \vdash (a, b) : \Sigma x{:}^q A.B}$$

T-Spread

$$\frac{\begin{array}{c}A = \Sigma x{:}^q A_1.A_2 \\ \Delta; \Gamma_1 \vdash a : A \\ \Delta, x{:}A_1; \Gamma_2, x{:}^q A_1 \vdash b : \Pi y :^1 A_2.B\{(x, y)/z\} \\ \Delta, z{:}A; \Gamma_3, z{:}^r A \vdash B : \mathbf{type}\end{array}}{\Delta; \Gamma_1 + \Gamma_2 \vdash \mathbf{spread}\, a\, \mathbf{to}\, x\, \mathbf{in}\, b : B\{a/z\}}$$

T-With

$$\frac{\begin{array}{c}\Delta; \Gamma_1 \vdash A : \mathbf{type} \\ \Delta, x{:}A; \Gamma_2, x{:}^r A \vdash B : \mathbf{type}\end{array}}{\Delta; \Gamma_1 + \Gamma_2 \vdash (x : A) \& B : \mathbf{type}}$$

T-Pair

$$\frac{\begin{array}{c}\Delta; \Gamma \vdash a : A \\ \Delta; \Gamma \vdash b : B\{a/x\} \\ \Delta, x{:}A; \Gamma_2, x{:}^r A \vdash B : \mathbf{type}\end{array}}{\Delta; \Gamma \vdash \&(a, b) : (x : A) \& B}$$

T-Prj1

$$\frac{\Delta; \Gamma \vdash a : (x : A) \& B}{\Delta; \Gamma \vdash \mathbf{prj}_1\, a : A}$$

T-Prj2

$$\frac{\Delta; \Gamma \vdash a : (x : A) \& B}{\Delta; \Gamma \vdash \mathbf{prj}_2\, a : B\{\mathbf{prj}_1\, a/x\}}$$