# System Specification

October 7, 2020

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

This document is intended to specify, in a readable form, the subject of the proofs in Section 6.2 of POPL paper 408 as well as explain the slight differences between the ott source file, this rendering, the POPL 408 submission, and the generated Coq files `dqtt.v` and `dqtt_inf.v`.

The reason for these slight differences is due to the restrictions of the Ott locally nameless backend and the LNgen theory generation tool.

1. All parts of the syntax must be defined concretely in the Ott source file.
2. All syntactic forms must bind at most one variable in each term.

The first limitation is simple to accommodate through minor edits of the outputs of Ott and LNgen.

The second limitation causes difficulty for the formalization of tensor products. The usual pattern matching elimination rule binds two variables, one for each component of the tuple. Therefore, compared to the syntax shown in the paper, we replace the pattern matching elimination form for $\Sigma$ types with a slightly more general, but less familiar, form.

Instead, we use an elimination form called "spread" of the form

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

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

$$\mathbf{let}\, (x, y)\, =\, (a : \Sigma x{:}^q A.B)\ \mathbf{in}\ b$$

using the term

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

# 1 Grammar

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

# 2 Step relation

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

$$\frac{a \rightsquigarrow a'}{a\ b \rightsquigarrow a'\ b}\ \text{S-AppCong} \qquad \frac{}{(\lambda x :^q A.a)\ b \rightsquigarrow a\{b/x\}}\ \text{S-Beta}$$

$$\frac{a \rightsquigarrow a'}{\mathbf{let\,unit}\ =\ a\ \mathbf{in}\ b \rightsquigarrow \mathbf{let\,unit}\ =\ a'\ \mathbf{in}\ b}\ \text{S-UnitCong} \qquad \frac{}{\mathbf{let\,unit}\ =\ \mathbf{unit}\ \mathbf{in}\ b \rightsquigarrow b}\ \text{S-UnitBeta}$$

S-BoxCong

$$\frac{a \rightsquigarrow a'}{\mathbf{let\,box}\, x \;=\; a \;\mathbf{in}\; b \rightsquigarrow \mathbf{let\,box}\, x \;=\; a' \;\mathbf{in}\; b}$$

S-BoxBeta

$$\frac{}{\mathbf{let\,box}\, x \;=\; \mathbf{box}_q\; a \;\mathbf{in}\; b \rightsquigarrow b\{a/x\}}$$

S-CaseCong

$$\frac{a \rightsquigarrow a'}{\mathbf{case}_q\; a\; \mathbf{of}\; b_1; b_2 \rightsquigarrow \mathbf{case}_q\; a'\; \mathbf{of}\; b_1; b_2}$$

S-Case1Beta

$$\frac{}{\mathbf{case}_q\; (\mathbf{inj}_1\; a)\; \mathbf{of}\; b_1; b_2 \rightsquigarrow b_1\; a}$$

S-Case2Beta

$$\frac{}{\mathbf{case}_q\; (\mathbf{inj}_2\; a)\; \mathbf{of}\; b_1; b_2 \rightsquigarrow b_2\; a}$$

S-SpreadCong

$$\frac{a \rightsquigarrow a'}{\mathbf{spread}\; a\; \mathbf{to}\; x\; \mathbf{in}\; b \rightsquigarrow \mathbf{spread}\; a'\; \mathbf{to}\; x\; \mathbf{in}\; b}$$

S-SpreadBeta

$$\frac{}{\mathbf{spread}\; (a_0, a_1)\; \mathbf{to}\; x\; \mathbf{in}\; b \rightsquigarrow b\{a_0/x\}\; a_1}$$

# 3 Typing relation

Another issue with $\Sigma$ 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

$$\frac{\Delta; \Gamma_1 \vdash a : A \qquad \Delta; \Gamma_1 \leq \Gamma_2}{\Delta; \Gamma_2 \vdash a : A}$$

T-type

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

T-var

$$\frac{x \notin \mathsf{dom}\, \Delta \qquad \Delta; \Gamma \vdash A : \mathbf{type}}{\Delta, x{:}A; 0 \cdot \Gamma, x{:}^1 A \vdash x : A}$$

T-weak

$$\frac{x \notin \mathsf{dom}\, \Delta \qquad \Delta; \Gamma_1 \vdash a : B \qquad \Delta; \Gamma_2 \vdash A : \mathbf{type}}{\Delta, x{:}A; \Gamma_1, x{:}^0 A \vdash a : B}$$

T-pi

$$\frac{\Delta; \Gamma_1 \vdash A : \mathbf{type} \qquad \Delta, x{:}A; \Gamma_2, x{:}^r A \vdash B : \mathbf{type}}{\Delta; \Gamma_1 + \Gamma_2 \vdash \Pi x :^q A.B : \mathbf{type}}$$

T-lam

$$\frac{\Delta, x{:}A; \Gamma_1, x{:}^q A \vdash a : B \qquad \Delta; \Gamma_2 \vdash A : \mathbf{type}}{\Delta; \Gamma_1 \vdash \lambda x :^q A.a : \Pi x :^q A.B}$$

T-app

$$\frac{\Delta; \Gamma_1 \vdash a : \Pi x :^q A.B \qquad \Delta; \Gamma_2 \vdash b : A}{\Delta; \Gamma_1 + q \cdot \Gamma_2 \vdash a\; b : B\{b/x\}}$$

T-CONV
$$\frac{\Delta;\Gamma_1 \vdash a : A \quad \Delta;\Gamma_2 \vdash B : \mathbf{type} \quad A \equiv B}{\Delta;\Gamma_1 \vdash a : B}$$

T-UNIT
$$\frac{}{\varnothing;\varnothing \vdash \mathbf{unit} : \mathbf{Unit}}$$

T-UNIT
$$\frac{}{\varnothing;\varnothing \vdash \mathbf{Unit} : \mathbf{type}}$$

T-UNITE
$$\frac{\Delta;\Gamma_1 \vdash a : \mathbf{Unit} \quad B_1 = B\{\mathbf{unit}/y\} \quad \Delta;\Gamma_2 \vdash b : B_1 \quad \Delta, y{:}\mathbf{Unit};\Gamma_3, y{:}^r\mathbf{Unit} \vdash B : \mathbf{type}}{\Delta;\Gamma_1 + \Gamma_2 \vdash \mathbf{let\,unit}\ =\ a\ \mathbf{in}\ b : B\{a/y\}}$$

T-BOX
$$\frac{\Delta;\Gamma \vdash A : \mathbf{type}}{\Delta;\Gamma \vdash \Box_q A : \mathbf{type}}$$

T-BOX
$$\frac{\Delta;\Gamma \vdash a : A}{\Delta;\ q\cdot\Gamma \vdash \mathbf{box}_q\ a : \Box_q A}$$

T-LETBOX
$$\frac{\Delta;\Gamma_1 \vdash a : \Box_q A \quad \Delta, x{:}A;\Gamma_2, x{:}^q A \vdash b : B\{\mathbf{box}_q\, x/y\} \quad \Delta, y{:}\Box_q A;\Gamma_3, y{:}^r\Box_q A \vdash B : \mathbf{type}}{\Delta;\Gamma_1 + \Gamma_2 \vdash \mathbf{let\,box}\, x\ =\ a\ \mathbf{in}\ b : B\{a/y\}}$$

T-SUM
$$\frac{\Delta;\Gamma_1 \vdash A_1 : \mathbf{type} \quad \Delta;\Gamma_2 \vdash A_2 : \mathbf{type}}{\Delta;\Gamma_1 + \Gamma_2 \vdash A_1 \oplus A_2 : \mathbf{type}}$$

T-INJ1
$$\frac{\Delta;\Gamma \vdash a : A_1 \quad \Delta;\Gamma_1 \vdash A_2 : \mathbf{type}}{\Delta;\Gamma \vdash \mathbf{inj}_1\ a : A_1 \oplus A_2}$$

T-INJ2
$$\frac{\Delta;\Gamma \vdash a : A_2 \quad \Delta;\Gamma_1 \vdash A_1 : \mathbf{type}}{\Delta;\Gamma \vdash \mathbf{inj}_2\ a : A_1 \oplus A_2}$$

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

T-SIGMA
$$\frac{\Delta;\Gamma_1 \vdash A : \mathbf{type} \quad \Delta, x{:}A;\Gamma_2, x{:}^r A \vdash B : \mathbf{type}}{\Delta;\Gamma_1 + \Gamma_2 \vdash \Sigma x{:}^q A.B : \mathbf{type}}$$

T-TENSOR
$$\frac{\Delta;\Gamma_1 \vdash a : A \quad \Delta;\Gamma_2 \vdash b : B\{a/x\} \quad \Delta, x{:}A;\Gamma_3, x{:}^r A \vdash B : \mathbf{type}}{\Delta;\ q\cdot\Gamma_1 + \Gamma_2 \vdash (a, b) : \Sigma x{:}^q A.B}$$

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