Preservation Proof of $\mathbb{T}_{\{\cdot\}} + SAT_{\{\cdot\}}$

Maximiliano Cristiá
Universidad Nacional de Rosario and CIFASIS

Gianfranco Rossi
Università di Parma

April 2, 2022

Abstract

This document contains the preservation proof of $\mathbb{T}_{\{\cdot\}} + SAT_{\{\cdot\}}$. This proof is part of the proof of type safety of $\mathbb{T}_{\{\cdot\}} + SAT_{\{\cdot\}}$.

Contents

1 Conventions and notation

The proof is made for the rewrite rules of the following predicate symbols:

- $\{=\}$
- $\{\in, \mathit{un}, \|, \mathit{size}\}$
- $\{\mathit{id}, \mathit{inv}, \mathit{comp}\}$
- $\{\neq, \notin, \mathit{nsize}\}$

The proof for derived constraints (cf. Section 3.5 of the paper) is trivial as any derived constraint is defined through a formula containing only the above predicate symbols.

In each proof we assume the left hand side (l.h.s., i.e. the constraint being rewritten) of the rewrite rule is correctly typed and we prove that the right hand side (r.h.s.) is correctly typed by assigning a type for each new variable and using only the types appearing in the l.h.s. (that is we prove that $\mathcal{D}(t_1 : \tau_1;\ \ldots;\ t_k : \tau_k;\ v_1 : \tau'_1;\ \ldots, v_m : \tau'_m) \wedge \Phi$ is a well-typed formula).

Notational conventions

- l.h.s and r.h.s always refer to the sides of the current rewrite rule.
- When types τ, τ_i are mentioned in the proof, the correct statement is "there exist a type τ such that..." or an equivalent phrase. For instance:

  > If $\{t_1 \sqcup A\} \neq \{t_2 \sqcup B\}$ is correctly typed then both sets are of the same type: $\mathsf{set}(\tau)$.

  should be read as:

  > If $\{t_1 \sqcup A\} \neq \{t_2 \sqcup B\}$ is correctly typed then both sets are of the same type: $\mathsf{set}(\tau)$, *for some type* τ.

- Names in SmallCaps refer to rules in Figures 1 and 2 of the article.
- $A \subseteq B$ is equivalent to $\mathit{un}(A, B, B)$.
- Variable names n and N (possibly with sub and superscripts) are used to denote fresh variables.
- $\dot{x}$, for any name x, is a shorthand for x is a variable.

2 Equality

$$\begin{aligned}
&\{t_1, \ldots, t_m \sqcup \dot{A}\} = \{u_1, \ldots, u_n \sqcup \dot{A}\} \rightarrow \\
&\quad t_1 = u_j \wedge \{t_2, \ldots, t_m \sqcup \dot{A}\} = \{u_1, \ldots, u_{j-1}, u_{j+1}, \ldots, u_n \sqcup \dot{A}\} \\
&\quad \vee\ t_1 = u_j \wedge \{t_1, \ldots, t_m \sqcup \dot{A}\} = \{u_1, \ldots, u_{j-1}, u_{j+1}, \ldots, u_n \sqcup \dot{A}\} \\
&\quad \vee\ t_1 = u_j \wedge \{t_2, \ldots, t_m \sqcup \dot{A}\} = \{u_1, \ldots, u_n \sqcup \dot{A}\} \\
&\quad \vee\ \dot{A} = \{t_1 \sqcup N\} \wedge \{t_2, \ldots, t_m \sqcup N\} = \{u_1, \ldots, u_n \sqcup N\}
\end{aligned} \tag{2.1}$$

Proof. If $\{t_1, \ldots, t_m \sqcup \dot{A}\} = \{u_1, \ldots, u_n \sqcup \dot{A}\}$ is type correct then: (i) A is of type $\mathsf{set}(\tau)$, and (ii) $t_1, \ldots, t_m, u_1, \ldots, u_n$ are all of type τ. The first disjunct is proved as follows. $t_1 = u_j$ is correctly typed because both are of the same type by (ii); $\{t_2, \ldots, t_m \sqcup \dot{A}\} = \{u_1, \ldots, u_{j-1}, u_{j+1}, \ldots, u_n \sqcup \dot{A}\}$ is correctly typed as they are subsets of the sets at the left hand side. The second and third disjuncts are proved in the same way. In the last disjunct, N is assigned type $\mathsf{set}(\tau)$, then $A = \{t_1 \sqcup N\}$ is correctly typed by (i), (ii) and the type assigned to N; and $\{t_2, \ldots, t_m \sqcup N\} = \{u_1, \ldots, u_n \sqcup N\}$ is type correct because of (ii) and the type assigned to N. □

$$\begin{aligned}
&\{x \sqcup A\} = \{y \sqcup B\} \rightarrow \\
&\quad x = y \wedge A = B \\
&\quad \vee\ x = y \wedge \{x \sqcup A\} = B \\
&\quad \vee\ x = y \wedge A = \{y \sqcup B\} \\
&\quad \vee\ A = \{y \sqcup N\} \wedge \{x \sqcup N\} = B
\end{aligned} \tag{2.2}$$

Proof. This proof is in the paper. □

$$[k, m] = \varnothing \rightarrow m < k \tag{2.3}$$

Proof. If $[k, m] = \varnothing$ is type correct, then m and k are of type int and so $m < k$ is correctly typed. □

$$[k, m] = \{x \sqcup A\} \rightarrow \{x \sqcup A\} \subseteq [k, m] \wedge \mathit{size}(\{x \sqcup A\}, m - k + 1) \tag{2.4}$$

Proof. If $[k, m] = \{x \sqcup A\}$ is correctly typed then: (i) k, m are of type int, and (ii) $[k, m]$ and $\{x \sqcup A\}$ are of type $\mathsf{set}(\mathsf{int})$. Hence, $\{x \sqcup A\} \subseteq [k, m]$ is correctly typed, and (iii) $m - k + 1$ is of type int by (i). (i) and (ii) implies that $\mathit{size}(\{x \sqcup A\}, m - k + 1)$ is type correct (rule Sz). □

$$[k, m] = [i, j] \rightarrow (k \le m \wedge i \le j \wedge k = i \wedge m = j) \vee (m < k \wedge j < i) \tag{2.5}$$

Proof. If $[k,m]=[i,j]$ is correctly typed then k,m,i,j are of type int and so all the integer constraints are type correct. □

$$\begin{aligned}&\{t_1 \sqcup A\} \neq \{t_2 \sqcup B\} \rightarrow\\ &\quad n \in \{t_1 \sqcup A\} \wedge n \notin \{t_2 \sqcup B\}\\ &\quad \vee\, n \notin \{t_1 \sqcup A\} \wedge n \in \{t_2 \sqcup B\}\end{aligned} \tag{2.6}$$

Proof. If $\{t_1 \sqcup A\} \neq \{t_2 \sqcup B\}$ is correctly typed then both sets are of the same type: $\mathsf{set}(\tau)$. Hence, τ is the type assigned to n. In this case all the membership and not membership constraints at the right hand side are correctly typed. □

$$[k,m] \neq \varnothing \rightarrow k \leq m \tag{2.7}$$

Proof. If $[k,m] \neq \varnothing$ is correctly typed then k,m are of type int and so the arithmetic constraint at the right hand side is type correct. □

$$\begin{aligned}&[k,m] \neq [i,j] \rightarrow\\ &\quad (k \leq m \wedge (m \neq j \vee j < i \vee k \neq i)) \vee (i \leq j \wedge (m \neq j \vee m < k \vee k \neq i))\end{aligned} \tag{2.8}$$

Proof. If $[k,m] \neq [i,j]$ is correctly typed then k,m,i,j are of type int and so all the arithmetic constraints are type correct. □

3 Inequality

$$f(t_1,\dots,t_n) \neq f(u_1,\dots,u_n) \rightarrow t_1 \neq u_1 \vee \dots \vee t_n \neq u_n \tag{3.1}$$

where f is a $(\cdot,\cdot)$ or $\cdot ? \cdot$

Proof. If f is $(\cdot,\cdot)$ then the rule becomes

$$(t_1,t_2) \neq (u_1,u_2) \rightarrow t_1 \neq u_1 \vee t_2 \neq u_2$$

Now, if $(t_1,t_2) \neq (u_1,u_2)$ is well-typed then: (a) t_1,u_1 are of type τ_1; and (b) t_2,u_2 are of type τ_2. So, $t_1 \neq u_1$ well-type by a; and $t_2 \neq u_2$ is well-typed by (b).

If f is $\cdot ? \cdot$ then the rule becomes

$$t_1 ? t_2 \neq u_1 ? u_2 \rightarrow t_2 \neq u_2$$

Now, if $t_1 ? t_2 \neq u_1 ? u_2$ is well-typed then: (a) $t_1,u_1 \in \mathcal{B}$ and $t_1 = u_1$; and (b) $t_2,u_2 \in \mathcal{A}$. So, $t_2 \neq u_2$ is well-typed by (b). □

$$[k,m] \neq \varnothing \rightarrow k \leq m \tag{3.2}$$

Proof. If $[k, m] \neq \varnothing$ is correctly typed then k, m are of type int and so the integer constraint is well-typed. □

$$\begin{aligned}&[k, m] \neq [i, j] \rightarrow \\ &\quad (k \leq m \wedge (m \neq j \vee j < i \vee k \neq i)) \vee (i \leq j \wedge (m \neq j \vee m < k \vee k \neq i))\end{aligned} \tag{3.3}$$

Proof. If $[k, m] \neq [i, j]$ is correctly typed then k, m, i, j are of type int and so the integer constraints are well-typed. □

4 Membership

$$x \in \{y \sqcup A\} \rightarrow x = y \vee x \in A \tag{4.1}$$

Proof. If $x \in \{y \sqcup A\}$ is correctly typed then $\{y \sqcup A\}$ is of type $\mathsf{set}(\tau)$ and x and y are of type τ. Hence, $x = y$ and $x \in A$ are correctly typed by Eq and Mem, respectively. □

$$x \in \dot{A} \rightarrow \dot{A} = \{x \sqcup N\} \tag{4.2}$$

Proof. If $x \in A$ is correctly typed then A is of type $\mathsf{set}(\tau)$ and x is of type τ. Then, we assign $\mathsf{set}(\tau)$ as the type of N. In this case, $\dot{A} = \{x \sqcup N\}$. □

$$x \in [k, m] \rightarrow k \leq x \leq m \tag{4.3}$$

Proof. If $x \in [k, m]$ is correctly typed then x, k, m are of type int and so the integer constraint at the r.h.s. is type correct. □

5 Union

$$un(\dot{A}, \dot{A}, B) \rightarrow \dot{A} = B \tag{5.1}$$

Proof. If $un(\dot{A}, \dot{A}, B)$ is type correct then A and B are of the same type and so $\dot{A} = B$ is correctly typed. □

$$un(A, B, \varnothing) \rightarrow A = \varnothing \wedge B = \varnothing \tag{5.2}$$

Proof. If $un(A, B, \varnothing)$ is type correct then A and B are of the same set type and so $A = \varnothing$ and $B = \varnothing$ are correctly typed. □

$$un(\varnothing, A, \dot{B}) \rightarrow \dot{B} = A \tag{5.3}$$

Proof. If $un(\varnothing, A, \dot{B})$ is type correct then A and B are of the same type and so $\dot{B} = A$ is correctly typed. □

$$un(A, \varnothing, \dot{B}) \rightarrow \dot{B} = A \tag{5.4}$$

Proof. The proof is like the previous one. □

$$\begin{aligned}
&un(\{t \sqcup C\}, A, \dot{B}) \rightarrow \\
&\quad (t \notin A \land un(N_1, A, N) \\
&\quad\; \lor A = \{t \sqcup N_2\} \land un(N_1, N_2, N)) \\
&\quad\; \land \{t \sqcup C\} = \{t \sqcup N_1\} \land \dot{B} = \{t \sqcup N\}
\end{aligned} \tag{5.5}$$

Proof. If $un(\{t \sqcup C\}, A, \dot{B})$ is type correct then $C, A, \dot{B}$ are of type $\mathsf{set}(\tau)$ and t of type τ. Then $\mathsf{set}(\tau)$ is the type for N, N_1, N_2. In this way, $t \notin A$ is correctly typed because t of type τ and A is of type $\mathsf{set}(\tau)$; all the union constraints are correctly typed because all of their arguments are of type $\mathsf{set}(\tau)$; and the same holds for all the equality constraints. □

$$\begin{aligned}
&un(A, \{t \sqcup C\}, \dot{B}) \rightarrow \\
&\quad (t \notin A \land un(N_1, A, N) \\
&\quad\; \lor A = \{t \sqcup N_2\} \land un(N_1, N_2, N)) \\
&\quad\; \land \{t \sqcup C\} = \{t \sqcup N_1\} \land \dot{B} = \{t \sqcup N\}
\end{aligned} \tag{5.6}$$

Proof. Given that this rule is symmetric w.r.t. the previous one, the proof is similar. □

$$\begin{aligned}
&un(A, B, \{t \sqcup C\}) \rightarrow \\
&\quad (A = \{t \sqcup N_1\} \land un(N_1, B_2, N) \\
&\quad\; \lor B = \{t \sqcup N_1\} \land un(A, N_1, N) \\
&\quad\; \lor A = \{t \sqcup N_1\} \land B = \{t \sqcup N_2\} \land un(N_1, N_2, N)) \\
&\quad\; \land \{t \sqcup C\} = \{t \sqcup N\}
\end{aligned} \tag{5.7}$$

Proof. Given that this rule is symmetric w.r.t. the previous one, the proof is similar. □

$$\begin{aligned}
&un([k, m], A, B) \rightarrow \\
&\quad m < k \land A = B \\
&\quad \lor k \leq m \land \dot{N} \subseteq [k, m] \land size(\dot{N}, m - k + 1) \land un(\dot{N}, A, B)
\end{aligned} \tag{5.8}$$

Proof. If $un([k,m],A,B)$ is type correct then: (i) A,B are of type $\mathsf{set(int)}$; and (ii) k,m are of type int. We assign $\mathsf{set(int)}$ as the type for N. In turn, (ii) implies that all the arithmetic constraints are type correct and that (iii) $m-k+1$ is of type int. $A=B$ is type correct as both are of the same type by (i); $\dot{N} \subseteq [k,m]$ is type correct as both terms are of the same type by (i) and the type assigned to N); $un(\dot{N},A,B)$ is type correct because all the arguments have the same type by (i) and the type assigned to N; $size(\dot{N}, m-k+1)$ is type correct because of the type assigned to N and due to (iii). □

$$
\begin{aligned}
& un(A,[k,m],B) \rightarrow \\
& \quad m < k \land A = B \\
& \quad \lor\ k \leq m \land \dot{N} \subseteq [k,m] \land size(\dot{N}, m-k+1) \land un(A,\dot{N},B)
\end{aligned}
\tag{5.9}
$$

Proof. Given that this rule is symmetric w.r.t. the previous one, the proof is similar. □

$$
\begin{aligned}
& un(A,B,[k,m]) \rightarrow \\
& \quad m < k \land A = \varnothing \land B = \varnothing \\
& \quad \lor\ (k \leq m \land \dot{N} \subseteq [k,m] \land size(\dot{N}, m-k+1) \land un(A,B,\dot{N}))
\end{aligned}
\tag{5.10}
$$

Proof. Given that this rule is symmetric w.r.t. the previous one, the proof is similar. □

$$
\begin{aligned}
& un([k,m],[i,j],A) \rightarrow \\
& \quad (m < k \land j < i \land A = \varnothing) \\
& \quad \lor\ (m < k \land i \leq j \land [i,j] = A) \\
& \quad \lor\ (k \leq m \land j < i \land [k,m] = A) \\
& \quad \lor\ (k \leq m \land i \leq j \\
& \qquad \land\ \dot{N}_1 \subseteq [k,m] \land size(\dot{N}_1, m-k+1) \\
& \qquad \land\ \dot{N}_2 \subseteq [i,j] \land size(\dot{N}_2, j-i+1) \\
& \qquad \land\ un(\dot{N}_1,\dot{N}_2,A))
\end{aligned}
\tag{5.11}
$$

Proof. If $un([k,m],[i,j],A)$ type correct then: (i) k,m,i,j are of type *Itype*; and (ii) A is of type $\mathsf{set(int)}$. We assign $\mathsf{set(int)}$ as the type for N_1, N_2. Hence, (i) implies that all the integer constraints are correctly typed and that (iii) $m-k+1, j-i+1$ are of type int. Then: $A=\varnothing$ is type correct because A is of a set type by (ii); $[i,j]=A$ and $[k,m]=A$ are type correct because all of the terms are of the same type by (i) and rule Int; $\dot{N}_1 \subseteq [k,m]$ and $\dot{N}_2 \subseteq [i,j]$ are type correct because all of the terms are of the same type by (i) and rule Int; $size(\dot{N}_1, m-k+1)$ and $size(\dot{N}_2, j-i+1)$ are type correct because of the type assigned to N_1, N_2 and due to (iii); and $un(\dot{N}_1,\dot{N}_2,A)$ is type correct because all the arguments are of the same type by (ii) and the type assigned to N_1, N_2. □

$$\begin{aligned}
&un([k,m],A,[i,j]) \rightarrow \\
&\quad j < i \wedge [k,m] = A = \varnothing \\
&\quad \vee\ i \leq j \wedge m < k \wedge A = [i,j] \\
&\quad \vee\ k \leq m \wedge i \leq j \\
&\qquad \wedge\ \dot{N}_1 \subseteq [k,m] \wedge size(\dot{N}_1, m-k+1) \\
&\qquad \wedge\ \dot{N}_2 \subseteq [i,j] \wedge size(\dot{N}_2, j-i+1) \\
&\qquad \wedge\ un(\dot{N}_1, A, \dot{N}_2)
\end{aligned} \tag{5.12}$$

Proof. Given that this rule is symmetric w.r.t. the previous one, the proof is similar. □

$$\begin{aligned}
&un(A,[k,m],[i,j]) \rightarrow \\
&\quad j < i \wedge [k,m] = A = \varnothing \\
&\quad \vee\ i \leq j \wedge m < k \wedge A = [i,j] \\
&\quad \vee\ k \leq m \wedge i \leq j \\
&\qquad \wedge\ \dot{N}_1 \subseteq [k,m] \wedge size(\dot{N}_1, m-k+1) \\
&\qquad \wedge\ \dot{N}_2 \subseteq [i,j] \wedge size(\dot{N}_2, j-i+1) \\
&\qquad \wedge\ un(A, \dot{N}_1, \dot{N}_2)
\end{aligned} \tag{5.13}$$

Proof. Given that this rule is symmetric w.r.t. the previous one, the proof is similar. □

$$\begin{aligned}
&un([k,m],[i,j],[p,q]) \rightarrow \\
&\quad (m < k \wedge [i,j] = [p,q]) \\
&\quad \vee\ (j < i \wedge [k,m] = [p,q]) \\
&\quad \vee\ (k \leq m \wedge i \leq j \wedge k \leq i \wedge i \leq m+1 \wedge m \leq j \wedge p = k \wedge q = j) \\
&\quad \vee\ (k \leq m \wedge i \leq j \wedge k \leq i \wedge i \leq m+1 \wedge j < m \wedge p = k \wedge q = m) \\
&\quad \vee\ (k \leq m \wedge i \leq j \wedge i < k \wedge k \leq j+1 \wedge m \leq j \wedge p = i \wedge q = j) \\
&\quad \vee\ (k \leq m \wedge i \leq j \wedge i < k \wedge k \leq j+1 \wedge j < m \wedge p = i \wedge q = m)
\end{aligned} \tag{5.14}$$

Proof. If $un([k,m],[i,j],[p,q])$ is type correct then: (i) k,n,i,j,p,q are of type int, and (ii) $[k,m],[i,j],[p,q]$ are of type $\mathsf{set}(\mathsf{int})$. Hence, all the integer constraints are correctly typed by (i); and $[i,j] = [p,q]$ and $[k,m] = [p,q]$ are correctly typed by (ii). □

6 Disjointness

$$\dot{A} \parallel \dot{A} \rightarrow \dot{A} = \varnothing \tag{6.1}$$

Proof. If $\dot{A} \parallel \dot{A}$ is type correct then A is of some set type and so $\dot{A} = \varnothing$ is correctly typed. □

$$\{t \sqcup B\} \parallel \dot{A} \rightarrow t \notin \dot{A} \land \dot{A} \parallel B \tag{6.2}$$

Proof. If $\{t \sqcup B\} \parallel \dot{A}$ is correctly typed then: (i) A, B are of type $\mathsf{set}(\tau)$, and (ii) t is of type τ. Hence, $t \notin \dot{A}$ is well-typed by (i) and (ii), and $\dot{A} \parallel B$ is well-typed by (i). □

$$\dot{A} \parallel \{t \sqcup B\} \rightarrow t \notin \dot{A} \land \dot{A} \parallel B \tag{6.3}$$

Proof. Given that this rule is symmetric w.r.t. the previous one, the proof is similar. □

$$\{t_1 \sqcup A\} \parallel \{t_2 \sqcup B\} \rightarrow t_1 \neq t_2 \land t_1 \notin B \land t_2 \notin A \land A \parallel B \tag{6.4}$$

Proof. If $\{t_1 \sqcup A\} \parallel \{t_2 \sqcup B\}$ is well-typed then: : (i) A, B are of type $\mathsf{set}(\tau)$, and (ii) t_1, t_2 are of type τ. Hence, $t_1 \neq t_2$ is well-typed by (ii); $t_1 \notin B$ is well-typed by (i) and (ii); $t_2 \notin \dot{A}$ is well-typed by (i) and (ii), and $\dot{A} \parallel B$ is well-typed by (i). □

$$[k, m] \parallel [i, j] \rightarrow m < k \lor j < i \lor (k \leq m \land i \leq j \land (m < i \lor j < k)) \tag{6.5}$$

Proof. If $[k, m] \parallel [i, j]$ is well-typed then: k, m, i, j are of type int. Hence all the integer constraints are well-typed. □

$$\begin{aligned}&[k, m] \parallel A \rightarrow \\ &\quad m < k \lor (k \leq m \land \dot{N} \subseteq [k, m] \land \mathit{size}(\dot{N}, m - k + 1) \land \dot{N} \parallel A)\end{aligned} \tag{6.6}$$

Proof. If $[k, m] \parallel A$ is well-typed then: (i) $[k, m], A$ are of type $\mathsf{set}(\mathsf{int})$, and (ii) k, m are of type int. $\mathsf{set}(\mathsf{int})$ is the type assigned to N (iii). Then, all the integer constraints are well-typed; (iv) $m - k + 1$ is of type int; $\dot{N} \subseteq [k, m]$ is well-typed by (i) and (iii); $\mathit{size}(\dot{N}, m - k + 1)$ is well-typed by (iii) and (iv); and $\dot{N} \parallel A$ is well-typed by (iii) and (i). □

7 Size (set cardinality)

$$\mathit{size}(\varnothing, m) \rightarrow m = 0 \tag{7.1}$$

Proof. If $\mathit{size}(\varnothing, m)$ is well-typed then m is of type int and so $m = 0$ is well-typed. □

$$size(A, 0) \rightarrow A = \varnothing \tag{7.2}$$

Proof. If $size(A, 0)$ is well-typed then A is of type $\mathsf{set}(\tau)$ and so $A = \varnothing$ is well-typed. □

If e is a compound arithmetic expression:

$$size(A, e) \rightarrow size(A, \dot{n}) \wedge \dot{n} = e \wedge 0 \leq \dot{n} \tag{7.3}$$

Proof. If $size(A, e)$ is well-typed then: (i) A is of type $\mathsf{set}(\tau)$, and (ii) e is of type int. int is the type assigned to n (iii). Hence: $size(A, \dot{n})$ is type correct by (i) and (iii); $\dot{n} = e$ is type correct by (iii) and (ii); and $0 \leq \dot{n}$ is type correct by (iii). □

$$\begin{aligned} & size(\{x \sqcup A\}, m) \rightarrow \\ & \quad x \notin A \wedge m = 1 + \dot{n} \wedge size(A, \dot{n}) \wedge 0 \leq \dot{n} \\ & \quad \vee\ A = \{x \sqcup \dot{N}\} \wedge x \notin \dot{N} \wedge size(\dot{N}, m) \end{aligned} \tag{7.4}$$

Proof. If $size(\{x \sqcup A\}, m)$ is type correct then: (i) A is of type $\mathsf{set}(\tau)$, (ii) x is of type τ, and (iii) m is of type int. Types are assigned as follows: (iv) $\mathsf{set}(\tau)$ is to N, and (v) int to n. Now, $1 + n$ is of type int by (v), so $m = 1 + \dot{n}$ is well-typed by (iii). In turn, each constraint is well-typed as follows: $x \notin A$ by (i) and (ii); $size(A, \dot{n})$ by (i) and (v); $A = \{x \sqcup \dot{N}\}$ by (i), (ii) and (iv); $x \notin \dot{N}$ by (ii) and (iv); and $size(\dot{N}, m)$ by (iv) and (iii). □

$$size([k, m], p) \rightarrow (m < k \wedge p = 0) \vee (k \leq m \wedge p = m - k + 1) \tag{7.5}$$

Proof. If $size([k, m], p)$ is correctly typed then k, m, p are of type int and so all the integer constraints are well-typed. □

8 Identity

$$id(\varnothing, R) \rightarrow R = \varnothing \tag{8.1}$$

Proof. If $id(\varnothing, R)$ is type correct then R is of type $\mathsf{rel}(\tau, \tau)$ and so $R = \varnothing$ is well-typed. □

$$id(A, \varnothing) \rightarrow A = \varnothing \tag{8.2}$$

Proof. If $id(A, \varnothing)$ is type correct then A is of type $\mathsf{set}(\tau)$ and so $A = \varnothing$ is well-typed. □

$$id(\{x \sqcup A\}, R) \rightarrow R = \{(x, x) \sqcup N\} \wedge id(A, N) \tag{8.3}$$

Proof. If $id(\{x \sqcup A\}, R)$ is correctly typed then: (i) x is of type τ; (ii) A is of type $\mathsf{set}(\tau)$; and (iii) R is of type $\mathsf{rel}(\tau, \tau)$. Type $\mathsf{rel}(\tau, \tau)$ is assigned to N (iv). Hence: $R = \{(x, x) \sqcup N\}$ is type correct by (i), (iii) and (iv); and $id(A, N)$ is type correct by (ii) and (iv). □

$$id(A, \{(x, y) \sqcup R\}) \rightarrow x = y \wedge A = \{x \sqcup N\} \wedge id(N, R) \tag{8.4}$$

Proof. If $id(A, \{(x, y) \sqcup R\})$ is correctly typed then: (i) x, y are of type τ; (ii) A is of type $\mathsf{set}(\tau)$; and (iii) R is of type $\mathsf{rel}(\tau, \tau)$. Type $\mathsf{set}(\tau)$ is assigned to N (iv). Hence, constraints are well-typed as follows: $x = y$ by (i); $A = \{x \sqcup N\}$ by (i), (ii) and (iv); and $id(N, R)$ is type correct by (iii) and (iv). □

9 Inverse (converse)

$$inv(R, \varnothing) \rightarrow R = \varnothing \tag{9.1}$$

Proof. If $inv(R, \varnothing)$ is well-typed then R is of type $\mathsf{rel}(\tau_1, \tau_2)$ and so $R = \varnothing$ is well-typed. □

$$inv(\varnothing, S) \rightarrow S = \varnothing \tag{9.2}$$

Proof. Given that this rule is symmetric w.r.t. the previous one, the proof is similar. □

$$\begin{aligned} &inv(\dot{R}, \{(x_1, y_1), \dots, (x_n, y_n) \sqcup \dot{R}\}) \rightarrow \\ &\quad \dot{R} = \{(x_1, y_1), (y_1, x_1) \sqcup N\} \wedge inv(N, \{(x_2, y_2), \dots, (x_n, y_n) \sqcup N\}) \end{aligned} \tag{9.3}$$

Proof. If $inv(\dot{R}, \{(x_1, y_1), \dots, (x_n, y_n) \sqcup \dot{R}\})$ is correctly typed then: (a) R is of type $\mathsf{rel}(\tau, \tau)$; and (b) x_i, y_i are of type τ. (c) $\mathsf{rel}(\tau, \tau)$ is the type assigned to N. Then: $\dot{R} = \{(x_1, y_1), (y_1, x_1) \sqcup N\}$ is correctly typed by (a)-(c), Prod, Ext and Eq; and $inv(N, \{(x_2, y_2), \dots, (x_n, y_n) \sqcup N\})$ is type correct by (b), (c), Prod and Ext. □

$$\begin{aligned} &inv(\{(x_1, y_1), \dots, (x_n, y_n) \sqcup \dot{S}\}, \dot{S}) \rightarrow \\ &\quad \dot{S} = \{(x_1, y_1), (y_1, x_1) \sqcup N\} \wedge inv(\{(x_2, y_2), \dots, (x_n, y_n) \sqcup N\}, N) \end{aligned} \tag{9.4}$$

Proof. Given that this rule is symmetric w.r.t. the previous one, the proof is similar. □

$$
\begin{aligned}
&\mathit{inv}(\{(x_1, y_1), \dots, (x_n, y_n) \sqcup \dot{R}\}, \{(a_1, b_1), \dots, (a_m, b_m) \sqcup \dot{R}\}) \rightarrow \\
&\quad \{(y_1, x_1) \sqcup N_1\} = \{(a_1, b_1), \dots, (a_m, b_m)\} \\
&\qquad \land\ \mathit{un}(\dot{R}, N_1, N_2) \land \mathit{inv}(\{(x_2, y_2), \dots, (x_n, y_n) \sqcup \dot{R}\}, N_2) \\
&\quad \lor\ (y_1, x_1) \notin \{(a_1, b_1), \dots, (a_m, b_m)\} \land (x_1, y_1) \notin \{(a_1, b_1), \dots, (a_m, b_m)\} \\
&\qquad \land\ \dot{R} = \{(x_1, y_1), (y_1, x_1) \sqcup N\} \\
&\qquad \land\ ((y_1, x_1) \notin \{(x_1, y_1), \dots, (x_n, y_n)\} \\
&\qquad\qquad \land\ \mathit{inv}(\{(x_2, y_2), \dots, (x_n, y_n) \sqcup N\}, \{(a_1, b_1), \dots, (a_m, b_m) \sqcup N\}) \\
&\qquad\quad \lor\ \{(y_1, x_1) \sqcup N_3\} = \{(x_2, y_2), \dots, (x_n, y_n)\} \land \mathit{un}(N, N_3, N_4) \\
&\qquad\qquad \land\ \mathit{inv}(N_4, \{(a_1, b_1), \dots, (a_m, b_m) \sqcup N\})) \\
&\quad \lor\ (y_1, x_1) \notin \{(a_1, b_1), \dots, (a_m, b_m)\} \\
&\qquad \land\ \{(x_1, y_1) \sqcup N_5\} = \{(a_1, b_1), \dots, (a_m, b_m)\} \\
&\qquad \land\ \dot{R} = \{(y_1, x_1) \sqcup N\} \land \mathit{un}(N, N_5, N_6) \\
&\qquad \land\ \mathit{inv}(\{(x_2, y_2), \dots, (x_n, y_n) \sqcup N\}, N_6)
\end{aligned}
\tag{9.5}
$$

Proof. If $\mathit{inv}(\{(x_1, y_1), \dots, (x_n, y_n) \sqcup \dot{R}\}, \{(a_1, b_1), \dots, (a_m, b_m) \sqcup \dot{R}\})$ is correctly typed then: (a) R is of type $\mathsf{rel}(\tau, \tau)$; and (b) x_i, y_i, a_i, b_i are of type τ. (c) $\mathsf{rel}(\tau, \tau)$ is the type assigned to N, N_i. All three branches are proved in a similar way; we will do it only for the last one. Each constraint in the last branch is well-typed as follows: $(y_1, x_1) \notin \{(a_1, b_1), \dots, (a_m, b_m)\}$ by (b), Prod, Ext and Mem; $\{(x_1, y_1) \sqcup N_5\} = \{(a_1, b_1), \dots, (a_m, b_m)\}$ by (b), (c), Prod, Ext and Eq; $\dot{R} = \{(y_1, x_1) \sqcup N\}$ by (a)-(c), Prod, Ext and Eq; $\mathit{un}(N, N_5, N_6)$ by (c); and $\mathit{inv}(\{(x_2, y_2), \dots, (x_n, y_n) \sqcup N\}, N_6)$ by (b)-(c), Prod and Ext. □

$$
\mathit{inv}(R, \{(y, x) \sqcup S\}) \rightarrow R = \{(x, y) \sqcup N\} \land \mathit{inv}(N, S) \tag{9.6}
$$

Proof. If $\mathit{inv}(R, \{(y, x) \sqcup S\})$ is type correct then: (a) R is of type $\mathsf{rel}(\tau_1, \tau_2)$; (b) y is of type τ_2; (c) x is of type τ_1; and (d) S is of type $\mathsf{rel}(\tau_2, \tau_1)$. (e) $\mathsf{rel}(\tau_1, \tau_2)$ is the type assigned to N. Then: $R = \{(x, y) \sqcup N\}$ is correctly typed by (a)-(c), (e), Prod, Ext and Eq; and $\mathit{inv}(N, S)$ is type correct by (d) and (e). □

$$
\mathit{inv}(\{(x, y) \sqcup R\}, S) \rightarrow S = \{(y, x) \sqcup N\} \land \mathit{inv}(R, N) \tag{9.7}
$$

Proof. Given that this rule is symmetric w.r.t. the previous one, the proof is similar. □

10 Composition

$$
\mathit{comp}(\varnothing, S, T) \rightarrow T = \varnothing \tag{10.1}
$$

Proof. If $comp(\varnothing, S, T)$ is correctly typed then S is of type $\mathsf{rel}(\tau_2, \tau_3)$ and T is of type $\mathsf{rel}(\tau_1, \tau_3)$, which implies that $T = \varnothing$ is well-typed. □

$$comp(R, \varnothing, T) \rightarrow T = \varnothing \tag{10.2}$$

Proof. Given that this rule is symmetric w.r.t. the previous one, the proof is similar. □

$$comp(\{(x, u)\}, \{(t, z)\}, T) \rightarrow (u = t \wedge T = \{(x, z)\}) \vee (u \neq t \wedge T = \varnothing) \tag{10.3}$$

Proof. If $comp(\{(x, u)\}, \{(t, z)\}, T)$ is type correct then: (a) x is of type τ_1; (b) u, t are of type τ_2; (c) z is of type τ_3; and (d) T is of type $\mathsf{rel}(\tau_1, \tau_3)$. So each constraint is well-typed as follows: $u = t$ by (b); $T = \{(x, z)\}$ by (a), (c), (d), Prod and Ext; $u \neq t$ by (b); and $T = \varnothing$ by (d). □

$$\begin{aligned}
&comp(\{(x, u) \sqcup R\}, \{(t, z) \sqcup S\}, \varnothing) \rightarrow \\
&\qquad u \neq t \\
&\qquad \wedge\ comp(\{(x, u)\}, S, \varnothing) \wedge comp(R, \{(t, z)\}, \varnothing) \wedge comp(R, S, \varnothing)
\end{aligned} \tag{10.4}$$

Proof. If $comp(\{(x, u) \sqcup R\}, \{(t, z) \sqcup S\}, \varnothing)$ is type correct then: (a) x is of type τ_1; (b) u, t are of type τ_2; (c) z is of type τ_3; (d) R is of type $\mathsf{rel}(\tau_1, \tau_2)$; and (e) S is of type $\mathsf{rel}(\tau_2, \tau_3)$. So each constraint is well-typed as follows: $u \neq t$ by (b); $comp(\{(x, u)\}, S, \varnothing)$ by (a), (b), (e), Prod and Ext; $comp(R, \{(t, z)\}, \varnothing)$ by (b)-(d), Prod and Ext; and $comp(R, S, \varnothing)$ by (d)-(e). □

$$\begin{aligned}
&comp(\{(x, t) \sqcup R\}, \{(u, z) \sqcup S\}, \dot{T}) \rightarrow \\
&\qquad comp(\{(x, t)\}, \{(u, z)\}, N_1) \\
&\qquad \wedge\ comp(\{(x, t)\}, S, N_2) \wedge comp(R, \{(u, z)\}, N_3) \\
&\qquad \wedge\ comp(R, S, N_4) \\
&\qquad \wedge\ un(N_1, N_2, N_3, N_4, \dot{T})
\end{aligned} \tag{10.5}$$

$un(N_1, N_2, N_3, N_4, \dot{T})$ is a shorthand for $un(N_1, N_2, A) \wedge un(A, N_3, B) \wedge un(B, N_4, \dot{T})$, for some A and B (of the same type than N_i and T).

Proof. If $comp(\{(x, t) \sqcup R\}, \{(u, z) \sqcup S\}, \dot{T})$ is well-typed then: (a) x is of type τ_1; (b) u, t are of type τ_2; (c) z is of type τ_3; (d) R is of type $\mathsf{rel}(\tau_1, \tau_2)$; (e) S is of type $\mathsf{rel}(\tau_2, \tau_3)$; and (f) T is of type $\mathsf{rel}(\tau_1, \tau_3)$. (g) $\mathsf{rel}(\tau_1, \tau_3)$ is the type assigned to N_1, N_2, N_3, N_4. So each constraint is well-typed as follows: $comp(\{(x, t)\}, \{(u, z)\}, N_1)$ by (a)-(c) and (g); $comp(\{(x, t)\}, S, N_2)$ by (a), (b), (e) and (g); $comp(R, \{(u, z)\}, N_3)$ by (b)-(d) and (g); $comp(R, S, N_4)$ by (d), (e) and (g); and $un(N_1, N_2, N_3, N_4, \dot{T})$ by (f) and (g). □

$$\begin{aligned}&\mathit{comp}(R, S, \{(x,z) \sqcup T\}) \rightarrow\\&\qquad \mathit{un}(N_x, N_{rt}, R) \wedge \mathit{un}(N_z, N_{st}, S)\\&\qquad N_x = \{(x,n) \sqcup N_1\} \wedge N_z = \{(n,z) \sqcup N_2\}\\&\qquad \wedge\, \mathit{comp}(\{(x,x)\}, N_1, N_1) \wedge \mathit{comp}(N_2, \{(z,z)\}, N_2)\\&\qquad \wedge\, \mathit{comp}(N_x, N_{st}, N_3) \wedge \mathit{comp}(N_{rt}, N_z, N_4) \wedge \mathit{comp}(N_{rt}, N_{st}, N_5)\\&\qquad \wedge\, \mathit{un}(N_3, N_4, N_5, T)\end{aligned} \tag{10.6}$$

$\mathit{un}(N_3, N_4, N_5, T)$ is a shorthand for $\mathit{un}(N_3, N_4, A) \wedge \mathit{un}(A, N_5, T)$, for some A (of the same type than N_i and T).

Proof. If $\mathit{comp}(R, S, \{(x,z) \sqcup T\})$ is well-typed then: (a) R is of type $\mathsf{rel}(\tau_1, \tau_2)$; (b) S is of type $\mathsf{rel}(\tau_2, \tau_3)$; (c) x is of type τ_1; (d) z is of type τ_3; and (e) T is of type $\mathsf{rel}(\tau_1, \tau_3)$. (f) $\mathsf{rel}(\tau_1, \tau_2)$ is the type assigned to N_x, N_{rt}, N_1; (g) $\mathsf{rel}(\tau_2, \tau_3)$ is the type assigned to N_z, N_{st}, N_2; (h) τ_2 is the type assigned to n; (i) $\mathsf{rel}(\tau_1, \tau_3)$ is the type assigned to N_3, N_4, N_5. So each constraint is well-typed as follows: $\mathit{un}(N_x, N_{rt}, R)$ by (a) and (f); $\mathit{un}(N_z, N_{st}, S)$ by (b) and (g); $N_x = \{(x,n) \sqcup N_1\}$ by (f), (c) and (h); $N_z = \{(n,z) \sqcup N_2\}$ by (g), (h) and (d); $\mathit{comp}(\{(x,x)\}, N_1, N_1)$ by (c) and (f); $\mathit{comp}(N_2, \{(z,z)\}, N_2)$ by (d) and (g); $\mathit{comp}(N_x, N_{st}, N_3)$ by (f), (g) and (i); $\mathit{comp}(N_{rt}, N_z, N_4)$ by (f), (g) and (i); $\mathit{comp}(N_{rt}, N_{st}, N_5)$ by (f), (g) and (i); and $\mathit{un}(N_3, N_4, N_5, T)$ by (i) and (e). □

11 Not membership

$$x \notin \{y \sqcup A\} \rightarrow x \neq y \wedge x \notin A \tag{11.1}$$

Proof. If $x \notin \{y \sqcup A\}$ is correctly typed then $\{y \sqcup A\}$ is of type $\mathsf{set}(\tau)$ and x, y are of type τ. Hence, $x \neq y$ and $x \notin A$ are correctly typed by Eq and Mem, respectively. □

$$x \notin [k, m] \rightarrow x < k \vee m < x \tag{11.2}$$

Proof. If $x \notin [k, m]$ is correctly typed then x, k, m are of type int and so the integer constraints at the r.h.s. are type correct. □

12 Not size (not set cardinality)

$$\mathit{nsize}([k, m], p) \rightarrow (m < k \wedge p \neq 0) \vee (k \leq m \wedge p \neq m - k + 1) \tag{12.1}$$

Proof. If $\mathit{nsize}([k, m], p)$ is correctly typed then k, m, p are of type int and so all the integer constraints are well-typed. □

$$\mathit{nsize}(A, p) \rightarrow \mathit{size}(A, n) \wedge n \neq p \tag{12.2}$$

Proof. If $nsize(A, p)$ is well-typed then: (a) A is of type $\mathsf{set}(\tau)$; and (b) p is of type int. (c) The type assigned to n is int. Then $size(A, n)$ is well-typed too by (a) and (c); and $n \neq p$ is type correct by (b) and (c). □