Exercise 1. [20 pts]

Case: $\overline{\texttt{succ}\ (\texttt{pred}\ t) \to t}$

In this case, the same term can have different canonical terms. For instance, take "$\texttt{succ}\ (\texttt{pred}\ z)$". This can step to either:

- "z" Using the new rule
- "$\texttt{succ}\ z$" Using E-SUCC and E-PRED-ZERO

We can immediately recognize that both terms are in normal form and different, which is disastrous.

Case: $\overline{\texttt{iszero}\ (\texttt{succ}\ t) \to t}$

While the system might be confluent, the system is no longer deterministic. For instance, take "$\texttt{iszero}\ (\texttt{succ}\ (\texttt{pred}\ z))$". which can step to either:

- "$\texttt{false}$" using the new rule
- "$\texttt{iszero}\ (\texttt{succ}\ z)$" using E-ISZERO and E-PRED-ZERO

However, we also have that non-sensical terms step to sensical terms. For instance, we have "$\texttt{iszero}\ (\texttt{succ}\ \texttt{false})$", which is non-sensical, that steps to "$\texttt{false}$"

Exercise 2. [20 pts]

Theorem 1. *If v is a value and $\mathcal{D} : v \to^* v'$, then $v = v'$.*

Proof. By structural induction on $\mathcal{D}$

Case. $\mathcal{D} = \dfrac{}{v \to^* v}\ \texttt{refl}$

$v' = v$ by $\texttt{refl}$

Case. $\mathcal{D} = \dfrac{\begin{matrix}\mathcal{D}_1 \\ v \to^* s\end{matrix} \qquad \begin{matrix}\mathcal{D}_2 \\ s \to^* t\end{matrix}}{v \to^* t}\ \texttt{trans}$

$s = v$ by i.h. on $\mathcal{D}_1$

$t = v$ by i.h. on $\mathcal{D}_2$ with $s = v$ a value

Case. $\mathcal{D} = \dfrac{\begin{matrix}\mathcal{D}_0 \\ v \to t\end{matrix}}{v \to^* t}$ `single`

We proceed by induction to show there is no valid on $\mathcal{D}_0$

Subcase. $v = z$

z cannot step — By exhaustion of the rules

Subcase. $v = \texttt{succ}\ nv$

$\mathcal{D}_1 : nv$ cannot step — by i.h. on nv

`succ` nv cannot step — `E-SUCC` only valid rule and $\mathcal{D}_1$

□

Exercise 3. [20 pts]

Lemma 1. *Let $\mathcal{D} : t_1 \Rightarrow^* t_2$ and $\mathcal{E} : t_2 \Rightarrow^* t_3$. Then $t_1 \Rightarrow^* t_3$.*

Proof. By induction on $\mathcal{D}$

Case. $\mathcal{D} = \dfrac{}{t_1 \Rightarrow^* t_1}$ `m-refl`

$t_2 = t_1$ — by `m-refl`

$\mathcal{E} : t_1 \Rightarrow^* t_3$ — by above

Case. $\mathcal{D} = \dfrac{\begin{matrix}\mathcal{D}_1 \\ t_1 \Rightarrow^* s\end{matrix}\ c \qquad \begin{matrix}\mathcal{D}_2 \\ s \Rightarrow^* t_2\end{matrix}\ c}{t_1 \Rightarrow^* t_2}$ `m-step`

$\mathcal{F} : s \Rightarrow^* t_3$ — by i.h. with $\mathcal{D}_2$ and $\mathcal{E}$

$t_1 \Rightarrow^* t_3$ — by `m-step` with $\mathcal{D}_1$ and $\mathcal{F}$

□

Theorem 2. *If $\mathcal{D} : t \to^* s$, then $t \Rightarrow^* s$*

Proof. Proof by induction on $\mathcal{D}$.

Case. $\mathcal{D} = \dfrac{}{t \to^* t}$ `refl`

$t \Rightarrow^* t$ — by `m-refl`

Case. $\mathcal{D} = \dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2 \\ t \to^* r & r \to^* r\end{array}}{t \to^* s}\ \texttt{trans}$

$\mathcal{F}_1 : t \Rightarrow^* r$ by i.h. on $\mathcal{D}_1$

$\mathcal{F}_2 : r \Rightarrow^* s$ by i.h. on $\mathcal{D}_2$

$s \Rightarrow^* t$ by lemma with $\mathcal{F}_1$ and $\mathcal{F}_2$

Case. $\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}_0 \\ t \to s\end{array}}{t \to^* s}\ \texttt{single}$

$\mathcal{F} : s \Rightarrow^* s$ by `m-refl`

$t \Rightarrow^* s$ by `m-step` with $\mathcal{D}_0$ and $\mathcal{F}$

□

Theorem 3. *If $\mathcal{D} : t \Rightarrow^* s$, then $t \to^* s$*

Proof. Proof by induction on $\mathcal{D}$.

Case. $\mathcal{D} = \dfrac{}{t \Rightarrow^* t}\ \texttt{m-refl}$

$t \to^* t$ by `refl`

Case. $\mathcal{D} = \dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2 \\ t \to r & r \Rightarrow^* s\end{array}}{t \Rightarrow^* s}\ \texttt{m-step}$

$\mathcal{F}_1 : t \to^* r$ by `step` with $\mathcal{D}_1$

$\mathcal{F}_2 : r \to^* s$ by i.h. on $\mathcal{D}_2$

$t \to^* s$ by `trans` with $\mathcal{F}_1$ and $\mathcal{F}_2$

□

Exercise 4. [40 pts]

1. [5 pts]

$$\dfrac{}{\texttt{leq}\ z\ nv \to \texttt{true}}\ \texttt{E-LEQ-TRUE} \qquad \dfrac{}{\texttt{leq}\ (\texttt{succ}\ nv)\ z \to \texttt{false}}\ \texttt{E-LEQ-FALSE}$$

$$\dfrac{}{\texttt{leq}\ (\texttt{succ}\ nv_1)\ (\texttt{succ}\ nv_2) \to \texttt{leq}\ nv_1\ nv_2}\ \texttt{E-LEQ-SUCC}$$

$$\dfrac{t \to t'}{\texttt{leq}\ t\ s \to \texttt{leq}\ t'\ s}\ \texttt{E-LEQ-L} \qquad \dfrac{t \to t'}{\texttt{leq}\ nv\ t \to \texttt{leq}\ nv\ t'}\ \texttt{E-LEQ-R}$$

2. [16 pts]

Theorem 4. *Let $\mathcal{D} : t \to s$ and $\mathcal{E} : t \to r$, then $s = r$.*

Proof. Proof by structural induction on $\mathcal{D}$.

Case. $\mathcal{D} = \dfrac{}{\texttt{leq}\ z\ nv \to \texttt{true}}$ E-LEQ-TRUE

$t = \texttt{leq}\ z\ nv$ By $\mathcal{D}$

$s = \texttt{true}$ By$\mathcal{D}$

Let us now match on $\mathcal{E}$

SubCase. $\mathcal{E} = \dfrac{}{\texttt{leq}\ z\ nv \to \texttt{true}}$ E-LEQ-TRUE

$s = \texttt{true}$ By $\mathcal{E}$

SubCase. $\mathcal{E} = \dfrac{}{\texttt{leq}\ (\texttt{succ}\ nv')\ z \to \texttt{false}}$ E-LEQ-FALSE

Impossible This would imply $z = \texttt{succ}\ nv'$

SubCase. $\mathcal{E} = \dfrac{}{\texttt{leq}\ (\texttt{succ}\ nv_1)\ (\texttt{succ}\ nv_2) \to \texttt{leq}\ nv_1\ nv_2}$ E-LEQ-SUCC

Impossible This would imply $z = \texttt{succ}\ nv_1$

SubCase. $\mathcal{E} = \dfrac{t \to t'}{\texttt{leq}\ t\ s \to \texttt{leq}\ t'\ s}$ E-LEQ-L

Impossible This would imply $z \to t'$, but z is in normal form.

SubCase. $\mathcal{E} = \dfrac{t \to t'}{\texttt{leq}\ nv'\ t \to \texttt{leq}\ nv'\ t}$ E-LEQ-R

Impossible This would imply $nv \to t'$, but nv is in normal form.

Case. $\mathcal{D} = \dfrac{}{\texttt{leq}\ (\texttt{succ}\ nv)\ z \to \texttt{false}}$ E-LEQ-FALSE

$t = \texttt{leq}\ \texttt{succ}\ nv\ z$ By $\mathcal{D}$

$s = false$ By$\mathcal{D}$

Let us now match on $\mathcal{E}$

SubCase. $\mathcal{E} = \dfrac{}{\texttt{leq}\ z\ nv' \to \texttt{true}}$ E-LEQ-TRUE

Impossible This would imply $z = \texttt{succ}\ nv$

SubCase. $\mathcal{E} = \dfrac{}{\texttt{leq}\ (\texttt{succ}\ nv)\ z \to \texttt{false}}$ E-LEQ-FALSE

$s = \texttt{false}$ by $\mathcal{E}$

SubCase. $\mathcal{E} = \dfrac{}{\texttt{leq}\ (\texttt{succ}\ nv_1)\ (\texttt{succ}\ nv_2) \to \texttt{leq}\ nv_1\ nv_2}\ \texttt{E-LEQ-SUCC}$
Impossible This would imply $z = \texttt{succ}\ nv_2$

SubCase. $\mathcal{E} = \dfrac{t \to t'}{\texttt{leq}\ t\ s \to \texttt{leq}\ t'\ s}\ \texttt{E-LEQ-L}$
Impossible This would imply $\texttt{succ}\ nv \to t'$, but $\texttt{succ}\ nv$ is in normal form.

SubCase. $\mathcal{E} = \dfrac{t \to t'}{\texttt{leq}\ nv'\ t \to \texttt{leq}\ nv'\ t}\ \texttt{E-LEQ-R}$
Impossible This would imply $z \to t'$, but z is in normal form.

Case. $\mathcal{D} = \dfrac{}{\texttt{leq}\ (\texttt{succ}\ nv_1)\ (\texttt{succ}\ nv_2) \to \texttt{leq}\ nv_1\ nv_2}\ \texttt{E-LEQ-SUCC}$

$t = \texttt{leq}\ \texttt{succ}\ nv_1\ \texttt{succ}\ nv_2$ By $\mathcal{D}$
$s = \texttt{leq}\ nv_1\ nv_2$ By$\mathcal{D}$
Let us now match on $\mathcal{E}$

SubCase. $\mathcal{E} = \dfrac{}{\texttt{leq}\ z\ nv \to \texttt{true}}\ \texttt{E-LEQ-TRUE}$
Impossible This would imply $z = \texttt{succ}\ nv_1$

SubCase. $\mathcal{E} = \dfrac{}{\texttt{leq}\ (\texttt{succ}\ nv)\ z \to \texttt{false}}\ \texttt{E-LEQ-FALSE}$
Impossible This would imply $z = \texttt{succ}\ nv_2$

SubCase. $\mathcal{E} = \dfrac{}{\texttt{leq}\ (\texttt{succ}\ nv_1)\ (\texttt{succ}\ nv_2) \to \texttt{leq}\ nv_1\ nv_2}\ \texttt{E-LEQ-SUCC}$
$s = \texttt{leq}\ nv_1\ nv_2$ by $\mathcal{E}$

SubCase. $\mathcal{E} = \dfrac{t \to t'}{\texttt{leq}\ t\ s \to \texttt{leq}\ t'\ s}\ \texttt{E-LEQ-L}$
Impossible This would imply $\texttt{succ}\ nv_1 \to t'$, but $\texttt{succ}\ nv_1$ is in normal form.

SubCase. $\mathcal{E} = \dfrac{t \to t'}{\texttt{leq}\ nv\ t \to \texttt{leq}\ nv\ t}\ \texttt{E-LEQ-R}$
Impossible This would imply $\texttt{succ}\ nv_2 \to t'$, but $\texttt{succ}\ nv_2$ is in normal form.

Case. $\mathcal{D} = \dfrac{t \to t'}{\texttt{leq}\ t\ s \to \texttt{leq}\ t'\ s}$ `E-LEQ-L`

$t = \texttt{leq}\ t\ s$ By $\mathcal{D}$
$\mathcal{D}_0 : t \to t'$
$s = \texttt{leq}\ t'\ s$ By$\mathcal{D}$
Let us now match on $\mathcal{E}$

SubCase. $\mathcal{E} = \dfrac{}{\texttt{leq}\ z\ nv \to \texttt{true}}$ `E-LEQ-TRUE`
Impossible This would imply $z \to t'$

SubCase. $\mathcal{E} = \dfrac{}{\texttt{leq}\ (\texttt{succ}\ nv)\ z \to \texttt{false}}$ `E-LEQ-FALSE`
Impossible This would imply $\texttt{succ}\ nv \to t'$ but $\texttt{succ}\ nv$ is in normal form

SubCase. $\mathcal{E} = \dfrac{}{\texttt{leq}\ (\texttt{succ}\ nv_1)\ (\texttt{succ}\ nv_2) \to \texttt{leq}\ nv_1\ nv_2}$ `E-LEQ-SUCC`
Impossible This would imply $\texttt{succ}\ nv_1 \to t'$ but $\texttt{succ}\ nv_1$ is in normal form

SubCase. $\mathcal{E} = \dfrac{\genfrac{}{}{0pt}{}{\mathcal{E}_0}{t \to t''}}{\texttt{leq}\ t\ s \to \texttt{leq}\ t''\ s}$ `E-LEQ-L`
$t' = t''$ By i.h. on $\mathcal{D}_0$ and $\mathcal{E}_0$ $s = \texttt{leq}\ t'\ s$ by $\mathcal{E}$ and above

SubCase. $\mathcal{E} = \dfrac{r \to r'}{\texttt{leq}\ nv\ r \to \texttt{leq}\ nv\ r'}$ `E-LEQ-R`
Impossible This would imply $nv \to t'$, but nv is in normal form.

Case. $\mathcal{D} = \dfrac{t \to t'}{\texttt{leq}\ nv\ t \to \texttt{leq}\ nv\ t}$ `E-LEQ-R`

$t = \texttt{leq}\ t\ s$ By $\mathcal{D}$
$\mathcal{D}_0 : t \to t'$
$s = \texttt{leq}\ t'\ s$ By$\mathcal{D}$
Let us now match on $\mathcal{E}$

SubCase. $\mathcal{E} = \dfrac{}{\texttt{leq}\ z\ nv \to \texttt{true}}$ `E-LEQ-TRUE`
Impossible This would imply $nv \to t'$ but nv is in normal form

SubCase. $\mathcal{E} = \dfrac{}{\texttt{leq}\ (\texttt{succ}\ nv)\ z \to \texttt{false}}$ `E-LEQ-FALSE`
Impossible This would imply $z \to t'$ but z is in normal form

SubCase. $\mathcal{E} = \dfrac{}{\texttt{leq}\ (\texttt{succ}\ nv_1)\ (\texttt{succ}\ nv_2) \to \texttt{leq}\ nv_1\ nv_2}$ `E-LEQ-SUCC`

Impossible This would imply $\texttt{succ}\ nv_2 \to t'$ bu $\texttt{succ}\ nv_2$ is in normal form

SubCase. $\mathcal{E} = \dfrac{r \to r'}{\texttt{leq}\ r\ s \to \texttt{leq}\ r'\ s}$ `E-LEQ-L`

Impossible This would imply $nv \to r'$, but nv is in normal form.

SubCase. $\mathcal{E} = \dfrac{\begin{matrix}\mathcal{E}_0 \\ t \to t'\end{matrix}}{\texttt{leq}\ nv\ t \to \texttt{leq}\ nv\ t'}$ `E-LEQ-R`

$t' = t''$ By i.h. on $\mathcal{D}_0$ and $\mathcal{E}_0$ $s = \texttt{leq}\ nv\ t'$ by $\mathcal{E}$ and above

$\square$

3. [4 pts]

$$\frac{t_1 : \texttt{Nat} \quad t_2 : \texttt{Nat}}{\texttt{leq}\ t_1\ t_2 : \texttt{Bool}} \ \texttt{T-LEQ}$$

4. [15 pts]

Theorem 5. *If $\mathcal{D} : t \to t'$ and $\mathcal{E} : t : T$, then $t' : T$*

Proof. By induction on $\mathcal{D}$

Case. $\mathcal{D} = \dfrac{}{\texttt{leq}\ z\ nv \to \texttt{true}}$ `E-LEQ-TRUE`

$\texttt{leq}\ z\ nv : \texttt{Bool}$ by $\mathcal{E}$ and $T - LEQ$

$\texttt{true} : \texttt{Bool}$ by $T - TRUE$

Case. $\mathcal{D} = \dfrac{}{\texttt{leq}\ (\texttt{succ}\ nv)\ z \to \texttt{false}}$ `E-LEQ-FALSE`

$\texttt{leq}\ \texttt{succ}\ nv\ z : \texttt{Bool}$ by $\mathcal{E}$ and $T - LEQ$

$\texttt{false} : \texttt{Bool}$ by $T - FALSE$

Case. $\mathcal{D} = \dfrac{}{\texttt{leq}\ (\texttt{succ}\ nv_1)\ (\texttt{succ}\ nv_2) \to \texttt{leq}\ nv_1\ nv_2}$ `E-LEQ-SUCC`

$\texttt{leq}\ \texttt{succ}\ nv_1\ \texttt{succ}\ nv_2 : \texttt{Bool}$ by $\mathcal{E}$ and $T - LEQ$

$\texttt{succ}\ nv_1 : \texttt{Nat}$

$\texttt{succ}\ nv_2 : \texttt{Nat}$ by inversion on $T - LEQ$

$nv_1 : \texttt{Nat}$

$nv_2 : \texttt{Nat}$ by inversion on $T - SUCC$

$\texttt{leq}\ nv_1\ nv_2 : \texttt{Bool}$ by above and $T - LEQ$

$$\textbf{Case.}\quad \mathcal{D} = \cfrac{\begin{array}{c}\mathcal{E}_0\\ r \to r'\end{array}}{\texttt{leq}\ r\ s \to \texttt{leq}\ r'\ s}\ \texttt{E-LEQ-L}$$

$\texttt{leq}\ r\ s : \texttt{Bool}$ — by $\mathcal{E}$ and $T - LEQ$
$r : \texttt{Nat}$
$s : \texttt{Nat}$ — by inversion on $T - LEQ$
$r' : \texttt{Nat}$ — by i.h. on $\mathcal{E}$ and above
$\texttt{leq}\ r'\ s : \texttt{Bool}$ — by $T - LEQ$ and above

$$\textbf{Case.}\quad \mathcal{D} = \cfrac{\begin{array}{c}\mathcal{E}_0\\ t \to t'\end{array}}{\texttt{leq}\ nv\ t \to \texttt{leq}\ nv\ t'}\ \texttt{E-LEQ-R}$$

$\texttt{leq}\ nv\ t : \texttt{Bool}$ — by $\mathcal{E}$ and $T - LEQ$
$nv : \texttt{Nat}$
$t : \texttt{Nat}$ — by inversion on $T - LEQ$
$t' : \texttt{Nat}$ — by i.h. on $\mathcal{E}$ and above
$\texttt{leq}\ nv\ t' : \texttt{Bool}$ — by $T - LEQ$ and above

$\square$