COMPSCI 3MI3

Assignment 3

1 Solution Set

1.1 Q1

We assume the syntax and semantics for UAE as defined in the slides for topic 4. We define a new addition operator with the following syntax in EBNF:

```
t ::= ...
      | add t t

v ::= ...

nv ::= ...
```

Where `t` define terms, `v` values and `nv` numerical values as given in the slides. We add our addition operator to the definition of `t`.
We define the small-step semantics for the new addition operator by the following inference rules:

$$\texttt{add 0 nv} \rightarrow \texttt{nv}$$

$$\texttt{add (succ nv}_1\texttt{) nv}_2 \rightarrow \texttt{succ (add nv}_1\ \texttt{nv}_2\texttt{)}$$

$$\frac{t_1 \rightarrow t_1'}{\texttt{add}\ t_1\ t_2 \rightarrow\ \texttt{add}\ t_1'\ t_2}$$

$$\frac{t \rightarrow t'}{\texttt{add nv}\ t \rightarrow\ \texttt{add nv}\ t'}$$

1.2 Q2

We will prove that our language UAE as defined in the topic 4 slides is determinate. Thus, the extension of our language with the added semantics for arithmetic expression should satisfy the property

$$t \to t' \wedge t \to t'' \implies t' = t''$$

for all terms t, t', t''. We will prove this property holds by induction on the derivation $t \to t'$.

Base case. The base case denotes the final derivation where $t \to t'$ will yield a value instead of an expression evaluatable by a sub-derivation. The possible derivations that could yield a value are of the following:

Case: E-IfTrue, E-IfFalse
We can extend the argument presented in the slides for topic 4 to also hold for the new rules introduced with arithmetic expressions. It's obvious that none of the arithmetic derivations apply to terms of the form `if t1 then t2 else t3`, thus we need only to contend with the boolean subset of rules, which was already shown holds from topic 4.

Case: E-PredZero, E-PredSucc, E-IsZeroZero, E-IsZeroSucc
We can show that the derivations $t \to t'$ and $t \to t''$ must use the same rule, E-PredZero by comparing the term `pred` is applied to. `pred` is applied to `0`, a value, thus it cannot be further evaluated and must the final step, eliminating any rules that require sub-derivations. Furthermore, `0` cannot be evaluated to `succ nv` for any numerical value `nv`, and vice versa, since they are both values. Thus we can conlcude that E-PredZero is the only derivation that can applied to t.
We can apply a similar argument for E-PredSucc, E-IsZeroZero and E-IsZeroSucc.

Induction Step. We assume that for all sub-derviations of $t \to t'$ the above property holds, i.e. all sub-derivations are deterministic. We will prove that for all possible derivations $t \to t'$ the property holds. The derivation $t \to t'$ must be one of the following:

Case: E-IfTrue, E-IfFalse, E-If
We've already proved in class that for all derivations E-IfTrue, E-IfFalse and E-If over boolean elements our property of determinancy holds as shown in slides from topic 4. It is obvious that derivations added by extending our language over arithmetic expressions do not apply to terms of the form `if t1 then t2 else t3`. Thus we can extend our proof as shown in topic 4 slides such that our property will still hold for E-IfTrue, E-IfFalse and E-If.

Case: E-Succ
If E-Succ was the last derivation, we know that t must be of the form `succ s` where `s` is

a term in our language. And that via E-Succ $t' =$ `succ s'`. We then have the premise that there exists some sub-derivation $s \to s'$.
It is trivially obvious that all other rules cannot be applied to t, since they do not apply to terms of the form `succ s`. Thus we know that via E-Succ $t'' =$ `succ s''` and we have the premise of the sub-derivation $s \to s''$.
In order to show that $t' = t''$ we need to show that $s' = s''$. By our induction hypothesis we know that our property holds for all sub-derivations of $t \to t'$. Thus we know that

$$s \to s' \land s \to s'' \implies s' = s''$$

Since we have our premises $s \to s'$ and $s \to s''$ we can conclude $s' = s''$. Thus, $t' = t''$. Therefore our property holds for the E-Succ case.

Case: E-PredZero
If E-PredZero was the last derivation, we know that t must be of the form `pred 0`.
In order for t' to not equal t'', we would need to apply a different rule to t than E-PredZero, thus we show that only E-PredZero can be applied to t.

It is trivially obvious that all other rules except E-Pred and E-PredSucc cannot be applied to t, since they do not apply to terms of the form `pred t`. E-PredSucc cannot be applied to t since `succ nv` cannot be evaluated to `0` since both are values (V). Similarly, E-Pred can only be applied if `t1` in its definition can be evaluated. Since in our case `t1 = 0` $\in V$ futher evaluation of `0` is impossible, thus we cannot apply E-Pred.

Therefore we can only apply the derivation E-PredZero to t and our property holds if the last derivation was E-PredZero.

Case: E-PredSucc
We can prove this case similarly to E-PredZero. If E-PredSucc was the last derivation, we know that t must be of the form `pred (succ nv)` where `nv` is a numeric value.

It is trivially obvious that all other rules except E-Pred cannot be applied to t, since they cannot apply to terms of the form `pred (succ nv)`. E-Pred can only be applied if `t1` in its definition can be evaluated. Since in our case `t1 = succ nv` $\in V$ futher evaluation of `succ nv` is impossible, thus we cannot apply E-Pred.

Therefore we can only apply the derivation E-PredSucc to t and our property holds if the last derivation was E-PredSucc.

Case: E-Pred
We can prove this case similarly to E-Succ. If E-Pred was the last derivation, we know that t must be of the form `pred s` where `s` is a term in our language. Via E-Pred we know that $t' =$ `pred s'` and we have the premise that there exists some sub-derivation $s \to s'$.

We can apply a similar argument used in the E-PredZero case to show that the only possible derivation that can applied to t is E-Pred. Thus we know that via E-Pred $t'' =$ `pred s''` with the premise of $s \to s''$.
In order to show that $t' = t''$ we also need to show $s' = s''$. By our induction hypothesis we know that our property $s \to s' \land s \to s'' \implies s' = s''$ holds for all sub-derivations of $t \to t'$. Since we have the premises $s \to s'$ and $s \to s''$ we can conclude $s' = s''$. Thus, $t' =$ `pred` $s' =$ `pred` $s'' = t''$.
Therefore our inductive step holds for case E-Pred.

Case: E-IsZeroZero
We can prove this case similarly to E-PredZero. If E-IsZeroZero was the last derivation, we know that t must be of the form `iszero 0`.

We'll show that only E-IsZeroZero can be applied to t. It is trivially obvious that all other rules except E-IsZeroZero and E-IsZeroSucc cannot be applied to t, since they do not apply to terms of the form `iszero t`. E-IsZeroSucc cannot be applied to t since `succ nv` cannot be evaluated to `0` since both are values. E-IsZeroZero can only be applied if `t1` in its definition can be evaluated. Since in our case `t1 = 0` $\in V$ futher evaluation of `0` is impossible, thus we cannot apply E-IsZeroZero.

Therefore we can only apply the derivation E-IsZeroZero to t and our property holds if the last derivation was E-IsZeroZero.

Case: E-IsZeroSucc
We can prove this case similarly to E-PredZero. If E-IsZeroSucc was the last derivation, we know that t must be of the form `iszero (succ nv)` where `nv` is a numeric value.

It is trivially obvious that all other rules except E-IsZero cannot be applied to t, since they cannot apply to terms of the form `iszero (succ nv)`. E-IsZero can only be applied if `t1` in its definition can be evaluated. Since in our case `t1 = succ nv` $\in V$ futher evaluation of `succ nv` is impossible.

Therefore we can only apply the derivation E-IsZeroSucc to t and our property holds if the last derivation was E-IsZeroSucc.

Case: E-IsZero
We can prove this case similarly to E-Pred. If E-IsZero was the last derivation, we know that t must be of the form `iszero s` where `s` is a term in our language. Via E-IsZero we know that $t' =$ `iszero s'` and we have the premise that there exists some sub-derivation $s \to s'$.
We can apply a similar argument used in the E-IsZeroZero case to show that the only possible derivation that can applied to t is E-IsZero. Thus we know that via E-IsZero $t'' =$ `iszero s''` with the premise of $s \to s''$.

In order to show that $t' = t''$ we also need to show $s' = s''$. By our induction hypothesis we know that our property $s \to s' \land s \to s'' \implies s' = s''$ holds for all sub-derivations of $t \to t'$. Since we have the premises $s \to s'$ and $s \to s''$ we can conclude $s' = s''$. Thus, $t' = \texttt{iszero}\ s' = \texttt{iszero}\ s'' = t''$.
Therefore our inductive step holds for case E-IsZero.

We have shown that for all possible derivations of $t \to t'$ the property holds. Therefore our induction step holds.

Thus, we've shown that our UAE language, extended with arithmetic expressions, is still determinate.