Types and Programming Languages (15-814), Fall 2018
Assignment 2: Products and Sums
(Sample Solutions)

Contact: 15-814 Course Staff
Due Tuesday, October 2, 2018

This assignment is due by 23:59 on the above date and it must be submitted electronically as a PDF file on Canvas. Please use the attached template to typeset your assignment and make sure to include your full name and Andrew ID. As before, problems marked “WB” are subject to the whiteboard policy; all other problems must be done individually.

We also make the two following requests. Please record the time spend on the homework assignment. It is difficult for us to judge how long this assignment will take. Please mark the questions that you discussed with classmates using the whiteboard policy. We would like to see how many of you take advantage of this and for which questions.

Lazy products

In class on Tuesday, we learned about eager products. When eliminating eager products, we first reduced the components from left to right until both were values. Only then did we deem the pair to be a value. This is because we wanted to simultaneously use both components in the case elimination form, and in a call-by-value semantics, variables should only ever be instantiated with values.

With lazy products, a pair of expressions is always a value. Instead of a case elimination form that simultaneously extracts both components of an ordered pair, lazy products have left and right projections that extract the single corresponding component from the pair. Before we can project out of a term that is not an ordered pair, we must first reduce that term until it becomes one.

In this part of the assignment, you will explore the dynamics for lazy products and prove various properties about them. We explore lazy products in the context
of the simple language we have seen so far. Its syntax, statics, and dynamics are given in the appendices.

We first extend our syntax:

\[
\begin{align*}
\tau ::= & \cdots \\
\tau_1 \& \tau_2 & \text{lazy product of } \tau_1 \text{ and } \tau_2 \\
\end{align*}
\]

\[
\begin{align*}
e ::= & \cdots \\
\langle e_1, e_2 \rangle & \text{ordered pair of } e_1 \text{ and } e_2 \\
e \cdot l & \text{left projection} \\
e \cdot r & \text{right projection}
\end{align*}
\]

The introduction rule for lazy pairs is:

\[
\begin{align*}
\Gamma \vdash e_1 : \tau_1 & \quad \Gamma \vdash e_2 : \tau_2 \\
\Gamma \vdash \langle e_1, e_2 \rangle : \tau_1 \& \tau_2
\end{align*}
\] (I-&)

Its elimination rules are:

\[
\begin{align*}
\Gamma \vdash e : \tau_1 \& \tau_2 & \quad \Gamma \vdash e : \tau_1 \& \tau_2 \\
\Gamma \vdash e \cdot l : \tau_1 & \quad \Gamma \vdash e \cdot r : \tau_2
\end{align*}
\] (E-&-L, E-&-R)

**Task 1** (10 points, WB). Give rules capturing the intended dynamics for lazy products. That is, give rules defining the judgments \( e \ val \) and \( e \mapsto e' \) for terms \( e \) of the form \( \langle e_1, e_2 \rangle \), \( e_0 \cdot l \), and \( e_0 \cdot r \). They should satisfy \( \langle e_1, e_2 \rangle \cdot l \mapsto^* e_1 \) and \( \langle e_1, e_2 \rangle \cdot r \mapsto^* e_2 \) and capture the intuitions we gave above.

**Solution 1:** Pairs are always values. We step under the projections until they reach a value, and which point we extract the appropriate component.

\[
\begin{align*}
\langle e_1, e_2 \rangle \ val & \quad \langle e_1, e_2 \rangle \ val \\
e \mapsto e' & \quad e \mapsto e' \\
\langle e_1, e_2 \rangle \cdot l \mapsto e_1 & \quad \langle e_1, e_2 \rangle \cdot r \mapsto e_2
\end{align*}
\] (=&-VAL, STEP-PROJ-1, STEP-PROJ-2)

**Task 2** (10 points, WB). State and prove the canonical forms theorem for lazy pairs. The statement should be of the following form: “if \( \cdot \vdash e : \tau_1 \& \tau_2 \) and \( e \ val \), then \( e \) is a term of the form(s) . . . ”.
**Solution 2:** The statement is: if $\cdot \vdash e : \tau_1 \& \tau_2$ and $e \text{ val}$, then $e$ is a term of the form $\langle e_1, e_2 \rangle$ with $\cdot \vdash e_i : \tau_i$. The proof is by induction the judgment $e \text{ val}$.

Case ($\&$-VAL). Then $e$ is $\langle e_1, e_2 \rangle$ for some $e_1$ and $e_2$. We proceed by induction on the derivation $\cdot \vdash \langle e_1, e_2 \rangle : \tau_1 \& \tau_2$. The only rule with a conclusion of this form is (I-&), and by inversion we get $\cdot \vdash e_i : \tau_i$.

Case ($\rightarrow$-VAL). Then $e$ is $\lambda x. e'$ for some $e'$. There are no typing rules with conclusions of the form $\cdot \vdash \lambda x. e' : \tau_1 \& \tau_2$, so this case is impossible.

Case (VAL/L). Then $e$ is $l \cdot e'$ for some $e'$. There are no typing rules with conclusions of the form $\cdot \vdash l \cdot e' : \tau_1 \& \tau_2$, so this case is impossible.

Case (VAL/R). Symmetric to (VAL/L).

Case (( )-VAL). Then $e$ is $( )$. There are no typing rules with conclusions of the form $\cdot \vdash ( ) : \tau_1 \& \tau_2$, so this case is impossible.

Case (PAIR-VAL). Then $e$ is $\langle e_1, e_2 \rangle$ for some $e_1$ and $e_2$. There are no typing rules with conclusions of the form $\cdot \vdash \langle e_1, e_2 \rangle : \tau_1 \& \tau_2$, so this case is impossible.

There are no other rules with conclusions of the form $e \text{ val}$, so this completes the proof. □

**Task 3** (10 points, WB). Show that the progress property still holds after the addition of lazy pairs. In particular, prove if $\cdot \vdash e : \tau$ by (I-&), (E-&-L), or (E-&-R), then either $e \text{ val}$ or there exists an $e'$ such that $e \rightarrow e'$.

**Solution 3:** We proceed by induction on the judgment $\cdot \vdash e : \tau$. All cases but the following are unchanged.

Case (I-&). Then $e$ is $\langle e_1, e_2 \rangle$ for some $e_1$ and $e_2$. We have $e \text{ val}$ by ($\&$-VAL).

Case (E-&-L). Then $\cdot \vdash e \cdot l : \tau_1$ for some $e$ such that $\cdot \vdash e : \tau_1 \& \tau_2$. By the induction hypothesis, either $e \text{ val}$ or $e \rightarrow e'$. In the first case, $e \equiv \langle e_1, e_2 \rangle$ by Task 2. Then $e \cdot l \rightarrow e_1$ by (STEP-PROJL-2). In the second case, $e \cdot l \rightarrow e' \cdot l$ by (STEP-PROJL-1).

Case (E-&-R). Symmetric to the previous case. □

**Task 4** (5 points, WB). Show that the preservation property still holds after the addition of lazy pairs. In particular, show that if $e \rightarrow e'$ by one of the rules you gave in task 1 and $\cdot \vdash e : \tau$, then $\cdot \vdash e' : \tau$.

**Solution 4:** We proceed by induction on the judgment $e \rightarrow e'$.

Case (STEP-PROJL-1). Then $e \cdot l \rightarrow e' \cdot l$ and $e \rightarrow e'$. The only rule with a conclusion of the form $\cdot \vdash e \cdot l : \tau$ is (E-&-L). By inversion, $\cdot \vdash e : \tau \& \tau_2$ for some $\tau_2$. By the induction hypothesis on $e \rightarrow e'$, we have $\cdot \vdash e' : \tau \& \tau_2$. By (E-&-L), we have $\cdot \vdash e' \cdot l : \tau$ as desired.

Case (STEP-PROJR-1). Symmetric to the previous case.

Case (STEP-PROJL-2). Then $\langle e_1, e_2 \rangle \cdot l \rightarrow e_1$. The only rule with a conclusion of the form $\cdot \vdash \langle e_1, e_2 \rangle \cdot l : \tau$ is (E-&-L). By inversion, $\cdot \vdash \langle e_1, e_2 \rangle : \tau \& \tau_2$ for some $\tau_2$. By inversion (rule (I-&)), $\cdot \vdash e_1 : \tau$, as desired.
Case (STEP-PROJ-R-2). Symmetric to the previous case.

Task 5 (5 points, WB). Write down terms $\xi$ and $\xi^{-1}$ such that

\[
\vdash \xi : \tau \otimes \sigma \rightarrow \tau \& \sigma \\
\vdash \xi^{-1} : \tau \& \sigma \rightarrow \tau \otimes \sigma
\]

and for all values $v$ of type $\tau \otimes \sigma$, $\xi^{-1}(\xi(v)) \rightarrow^* v$ (you do not need to prove this). Do these terms witness the isomorphism? If so, state this. If not, briefly explain why.

**Hint.** Consider the dynamics of eager and lazy products in the presence of non-termination.

**Solution 5:** Let $\xi : \tau \otimes \sigma \rightarrow \tau \& \sigma$ and $\xi^{-1} : \tau \& \sigma \rightarrow \tau \otimes \sigma$ be given by

\[
\xi = \lambda x. \text{case } x \{ (l, r) \Rightarrow \langle l, r \rangle \} \\
\xi^{-1} = \lambda x. \langle x \cdot l, x \cdot r \rangle
\]

By the canonical forms theorem in lecture 7, all values $v$ of type $\tau \otimes \sigma$ are of the form $\langle v_1, v_2 \rangle$ with $v_1$ a value of type $\tau$ and $v_2$ a value of type $\sigma$. Then for all such $\langle v_1, v_2 \rangle$,

\[
\xi^{-1}(\xi(\langle v_1, v_2 \rangle)) \equiv (\lambda x. \langle x \cdot l, x \cdot r \rangle)(\lambda x. \text{case } x \{ (l, r) \Rightarrow \langle l, r \rangle \})(v_1, v_2) \\
\quad \mapsto (\lambda x. \langle x \cdot l, x \cdot r \rangle)(\text{case } \langle v_1, v_2 \rangle \{ (l, r) \Rightarrow \langle l, r \rangle \}) \\
\quad \mapsto (\lambda x. \langle x \cdot l, x \cdot r \rangle)(\langle v_1, v_2 \rangle/l, r)\langle l, r \rangle) \\
\quad \equiv (\lambda x. \langle x \cdot l, x \cdot r \rangle)\langle v_1, v_2 \rangle \\
\quad \mapsto (\langle v_1, v_2 \rangle \cdot l, \langle v_1, v_2 \rangle \cdot r) \\
\quad \mapsto \langle v_1, v_2 \rangle.
\]

These mappings fail to establish an isomorphism for several reasons. First, $\langle |e_1, e_2| \rangle$ val even if $e_1$ diverges (does not reduce to a value). Then $\xi(\xi^{-1}(\langle e_1, e_2 \rangle))$ will diverge because $(\langle e, v \rangle \cdot l, \langle e_1, e_2 \rangle \cdot r)$ diverges and

\[
\xi(\xi^{-1}(\langle e_1, e_2 \rangle)) \equiv (\lambda x. \text{case } x \{ (l, r) \Rightarrow \langle l, r \rangle \})(\lambda x. \langle x \cdot l, x \cdot r \rangle)\langle e_1, e_2 \rangle) \\
\quad \mapsto (\lambda x. \text{case } x \{ (l, r) \Rightarrow \langle l, r \rangle \})\langle e_1, e_2 \rangle \cdot l, \langle e_1, e_2 \rangle \cdot r).
\]

Assume next that $e_1$ and $e_2$ converge to $v_1$ and $v_2$, respectively. In this case, $\xi(\xi^{-1}(\langle e_1, e_2 \rangle)) \rightarrow^* \langle v_1, v_2 \rangle$, and it is possible that $\langle e_1, e_2 \rangle \neq \langle v_1, v_2 \rangle$.

The assigned tasked also asked you to speculate on how we could modify the definition of mutual inverse so that $\xi$ and $\xi^{-1}$ became mutual inverses. This portion of the task was misguided because $\tau \otimes \sigma$ and $\tau \& \sigma$ are fundamentally
different types and should not be isomorphic. Indeed, it is laziness of \& that permits us to encode infinite streams, something impossible under the eagerness of \(\otimes\). A better formulation would have been “characterize the values \(v\) for which \(\xi(\xi^{-1}(v)) \mapsto^* v\)”. This portion of the task was ignored during grading.

A billion dollar mistake

A frequent source of bugs programs is attempting to dereference null pointers. Languages subject to this class of errors feature a type \(\pi\) of “pointers” with a distinguished pointer \texttt{null} called the “null pointer”. The intention is that the null pointer represent a lack of value, while all other pointers can be “dereferenced” to produce a value. Any attempt to dereference a null pointer is necessarily an error. This class of errors is so rampant that Hoare, the inventor of the null pointer, has called null pointers his “billion dollar mistake” [2].

The crux of the problem is a mis-identification of the type option type \(\pi\) \texttt{opt} with the type \(\pi\). The option type \(\tau\) \texttt{opt} represents optional values of type \(\tau\), where \texttt{some} \(e\) captures the presence of a value \(e\) of type \(\tau\) and \texttt{none} represents the lack of value. We can test for the presence of a value using the construction “\texttt{case} \(e_1\) \{ \texttt{some} \(x\) \(\Rightarrow\) \(e_2\) | \texttt{none} \(\Rightarrow\) \(e_3\)\}”. This checks if \(e_1\) is \texttt{none}, in which it produces \(e_3\), and if \(e_1\) is \texttt{some} \(v_1\), then we produce \([v_1/x]\) \(e_2\). This can be encoded using sum types as follows:

\[
\tau\texttt{opt} = \tau + 1
\]

\[
\texttt{some} \(e\) = l \cdot e
\]

\[
\texttt{none} = r \cdot \langle \rangle
\]

\[
\texttt{case} \ e_1\ \{ \texttt{some} \ x \Rightarrow e_2\ | \ \texttt{none} \Rightarrow e_3\\} = \texttt{case} \ e_1\ \{ l \cdot x \Rightarrow e_2\ | \ r \cdot \cdot \Rightarrow e_3\} \]

The key point is that the type system stops us from directly using an optional value \(e\) of type \(\tau\) \texttt{opt} in a context expecting a value of type \(\tau\): the type system forces us to account for the fact that \(e\) could be \texttt{none}. In contrast, \(\pi\) treats the null pointer \texttt{null} as a genuine pointer, allowing it to be used in any context expecting a genuine pointer.

The affected languages try to work around this problem by providing a function \texttt{isnull} : \(\pi\) \(\rightarrow\) \texttt{bool} that produces \texttt{true} if it is applied to \texttt{null}, and otherwise produces \texttt{false}. To avoid accidentally dereferencing a pointer, code is then littered with checks of the form:

\[
\text{if (isnull } e) \text{ then ...handle error... else ...do something...}
\]

Unfortunately, it is very easy to forget such a check and attempt to dereference the potentially \texttt{null} value \(e\). Implicitly, this work-around attempts to simulate
the type $\tau_{\text{opt}}$ using $\text{bool} \otimes \tau$, where a value of type $\tau$ is tagged with a boolean that signals whether or not the value is actually present. The reader is referred to [1, pp. 92f.] for more details.

**Task 6** (10 points, WB, [1, Ex. 11.2]). Informally show that we cannot identify $\text{bool} \otimes \tau$ and $\tau_{\text{opt}}$ for arbitrary $\tau$. Do so by attempting to give an implementation of $\tau_{\text{opt}}$ in terms of $\text{bool} \otimes \tau$ by sensibly completing the following chart:

- $\text{none} = ?$
- $\text{some } e = ?$
- $\text{case } e_1 \{ \text{some } x \Rightarrow e_2 \mid \text{none } \Rightarrow e_3 \} = ?$

Where do you get stuck if you do not additionally assume the existence of a "null" value $\text{null}_\tau$ for each type $\tau$? Argue that even by artificially assuming the existence of such values, you cannot complete the chart in a manner that captures the semantics of $\tau_{\text{opt}}$ in their absence. (Please be brief: your answer must contain at most eight lines of prose.)

For your convenience, you may assume the existence of an if $b$ then $e_1$ else $e_2$ construct as defined in lecture 6.

**Solution 6:** Without the existence of $\text{null}_\tau$, we get stuck when we try to implement $\text{none}$: we have no a priori means of conjuring a closed value of type $\tau$ for arbitrary $\tau$ (consider $\tau = 0$), but we need such a value for the second component of the pair. Using $\text{null}_\tau$, we could sensibly attempt to complete the chart as:

- $\text{none} = \langle \text{false}, \text{null}_\tau \rangle$
- $\text{some } e = \langle \text{true}, e \rangle$

  $\text{case } e_1 \{ \text{some } x \Rightarrow e_2 \mid \text{none } \Rightarrow e_3 \} = \text{case } e_1 \{ \langle b, v \rangle \Rightarrow$

  $\text{if } b \text{ then } (\lambda x. e_2) v \text{ else } e_3 \}.$

We could alternatively leverage the variable convention and use a binding trick:

  $\text{case } e_1 \{ \text{some } x \Rightarrow e_2 \mid \text{none } \Rightarrow e_3 \} = \text{case } e_1 \{ \langle b, x \rangle \Rightarrow$

  $\text{if } b \text{ then } e_2 \text{ else } e_3 \}.$

This fails to capture the semantics of $\tau_{\text{opt}}$ because we might attempt to case on $\langle \text{true}, \text{null}_\tau \rangle$. This pair has no corresponding genuine option type expression and the case expression steps to the illegal term $[\text{null}_\tau/x]e_2$. \qed
Gaining types

Task 7 (5 points, WB). Find terms $e$ and $e'$ and types $\tau$ and $\tau'$ such that $\cdot \vdash e : \tau$, $e \mapsto e'$, and $\cdot \vdash e : \tau'$, but not $\cdot \vdash e : \tau'$.

Solution 7: There were many creative solutions. Here are a few.
Consider $e = \text{case } l \cdot () \{ l \cdot x \Rightarrow l \cdot () | r \cdot x \Rightarrow r \cdot () \}$. Then $\cdot \vdash e : 1 + 1$ has a unique type, but $e \mapsto l \cdot ()$ and $\cdot \vdash l \cdot () : 1 + \tau$ for all $\tau$.
Consider $e = (\lambda f. \text{case } (f()) \{ () \Rightarrow f \}) (\lambda x.x)$. Then $\cdot \vdash e : 1 \rightarrow 1$ has a unique type, but $e \mapsto \text{case } ((\lambda x.x()) \{ () \Rightarrow \lambda x.x \})$, which has type $\tau \rightarrow \tau$ for all $\tau$.
Consider $e = \text{case } (r \cdot ()) \{ l \cdot \_ \Rightarrow \lambda f. \lambda x.f x | r \cdot \_ \Rightarrow \lambda x.x \}$. Then $\cdot \vdash e : (\alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha)$ but not $\cdot \vdash e : \alpha \rightarrow \alpha$. However, $e \mapsto \lambda x.x$, which has type $\tau \rightarrow \tau$ for all $\tau$. ☐

Is zero a zero?

Task 8 (5 points, WB). Is the nullary sum type $0$ is the zero for $\otimes$? That is, prove or disprove that for all $\tau$,
$$\tau \otimes 0 \cong 0.$$  
In the affirmative case, we only ask that you write down the two terms witnessing the isomorphism. In the negative case, you must provide a counter-example and explain why it is a counter-example.

Solution 8: The isomorphism is witnessed by the following terms:
$$\phi = \lambda x. \text{case } x \{ (_, z) \Rightarrow z \},$$
$$\phi^{-1} = \lambda x. \text{case } x \{ \}.$$  
There are no values of type $0$, nor of type $\tau \otimes 0$ by the canonical forms theorem for $\otimes$, so these two functions are vacuously mutual inverses. ☐

Task 9 (0 points). How long did you spend on this assignment? Please list the questions that you discussed with classmates using the whiteboard policy.
References
