Submit your modified `a5.rkt` by email (joshuad@cs.queensu.ca) as `a5-yourname.rkt`.

Note: Questions marked with a + are bonus questions. You can receive full marks without doing them.

**Types**

\[
S, T ::= \text{unit} \quad \text{unit type} \\
| \text{int} \quad \text{type of integers} \\
| \text{bool} \quad \text{type of booleans} \\
| S \rightarrow T \quad \text{type of functions on } S \text{ that produce } T \\
| S \times T \quad \text{type of pairs of one } S \text{ and one } T
\]

**Typing contexts**

\[
\Gamma ::= \emptyset \quad \text{empty context} \\
| \Gamma, x : S \quad \text{ } x \text{ has type } S
\]

\[
\Gamma \vdash e : T \quad \text{Under assumptions } \Gamma, \text{ expression } e \text{ has type } T
\]

| Rule | Type | \[
\begin{align*}
(x : S) \in \Gamma & \quad \text{type-assum} \\
\Gamma \vdash x : S & \\
\Gamma, x : S \vdash e : T & \quad \text{Intro} \\
\Gamma \vdash \text{Lam } x \, e : (S \rightarrow T) & \\
\Gamma \vdash \text{Call } e_1 \, e_2 : T & \quad \text{Elim} \\
\Gamma \vdash \text{Pair } e_1 \, e_2 : (S \times T) & \quad \text{Intro} \\
\Gamma \vdash \text{Proj } _1 e & : S & \quad \text{Elim } _1 \\
\Gamma \vdash \text{Proj } _2 e & : S & \quad \text{Elim } _2 \\
\Gamma \vdash \text{Abs } e & : S & \quad \text{Intro} \\
\Gamma, x : S \vdash e_1 : T & \quad \text{Intro} \\
\Gamma, x : S \vdash e_2 : T & \quad \text{Intro} \\
\Gamma \vdash e_1 \, e_2 : T & \quad \text{Intro} \\
\Gamma \vdash \text{It } e \, e_1 \, e_2 : T & \quad \text{Intro} \\
\Gamma \vdash \text{Rec } f \, e_1 : T & \quad \text{Intro} \\
\end{align*}
\]

**Figure 1** Typing with functions, integers, booleans, sums (unions), and pairs (structs)
1 Implementing Typing in Racket

Question 1. The file a5.rkt includes a Racket procedure typeof, intended to take a context $$\Gamma$$ and expression $$e$$ and either

- returns a type $$S$$ such that $$\Gamma \vdash e : S$$ according to the rules in Figure 1, or
- returns $$\#f$$ (Racket’s “false”), if there is no such type.

However, the typeof procedure is incomplete: the branches for Ite, Split and Rec always return $$\#f$$ instead of implementing the respective rules (type-ite, type-split, type-rec).

Try to understand the existing code in relation to the corresponding rules. The hardest part of implementing type-ite will probably be checking that the type returned for $$e_{\text{then}}$$ matches the type returned for $$e_{\text{else}}$$, so looking at the code for $$\to$$Elim may be helpful, because $$\to$$Elim has to check that the type returned for $$e_2$$ matches the domain $$S$$ of the type returned for $$e_1$$.

Also, the rule for Rec is fairly similar to the rule for Lam—both rules have one premise, and both rules add to the typing context in that premise.

[See a5sol.rkt.]

2 Emptiness (bonus)

With sadness, I had to add the argument type $$S$$ to the expression form Lam. Otherwise, the code wouldn’t know what type $$S$$ to give for $$x$$ in the context in the $$\to$$Intro premise $$\Gamma, x : S \vdash e : T$$.

Similarly, I had to include the type $$S$$ in the recursion expression Rec.

By accident, this allows something rather strange. On a3 we saw that the formula $$\neg A$$ can be simulated by the formula $$(A \supset \text{False})$$. We can translate this formula by replacing $$A$$ with $$S$$ and $$\supset$$ with $$\to$$, but how can we translate False? We can’t use the expression False because it is an expression, not a type.

To have a type that corresponds to the formula False, we need a new type, for which we will use the symbol $$\bot$$. There will be no values of type $$\bot$$, but there are expressions of this type.

Question 2(a)+. Design a single elimination rule for $$\bot$$ (based on FalseElim from a3).

Two valid approaches:

- Design a rule that has the same expression in both the premise and conclusion (sometimes called a stationary rule).

$$\begin{align*}
\Gamma \vdash e : \bot \\
\hline
\Gamma \vdash e : S
\end{align*}$$

- Design a rule that “focuses” on a subexpression of type $$\bot$$, using a new expression form.

$$\begin{align*}
\Gamma \vdash e_0 : \bot & \quad \Gamma \vdash e_1 : S \\
\hline
\Gamma \vdash (\text{Imposs } e_0 e_1) : S
\end{align*}$$

[The solution I had in mind was the first, stationary rule, but the second rule is also a reasonable approach.]
§2  Emptiness (bonus)

**Question 2(b).** Find an expression $e$ such that $\emptyset \vdash e : \bot$. Do not add an introduction rule for $\bot$! Your expression should have type $\bot$, in the empty context, using only the rules from Figure 1 (and possibly your $\bot$Elim, but that is unlikely to help since you are trying to find a “sneaky” way to introduce $\bot$, not to eliminate it).

$$e = (\text{Rec } x \bot x)$$

**Question 2(c).** Write the derivation showing that $\emptyset \vdash e : \bot$.

$$
\begin{align*}
(x : \bot) &\in (x : \bot) & \text{type-assum} \\
x : \bot &\vdash x : \bot & \text{type-assum} \\
\emptyset &\vdash (\text{Rec } x \bot x) : \bot & \text{type-rec}
\end{align*}
$$
3 Progress

For this question, we need the small-step semantics.

Expressions  

\[ e ::= () \mid (Rec \ x \ S \ e) \mid n \mid (+ \ e \ e) \mid (- \ e) \mid (Abs \ e) \mid True \mid False \mid (Ite \ e \ e \ e) \mid (= \ e \ e) \mid (< \ e \ e) \mid (Pair \ e) \mid (Proj_1 \ e) \mid (Proj_2 \ e) \mid (Split \ e \ (x \ x => e)) \]

Values  

\[ v ::= () \mid n \mid True \mid False \mid x \mid (Lam \ x \ S \ e) \mid (Pair \ v) \]

Contexts  

\[ C ::= [] \mid (+ \ C \ e) \mid (+ \ v \ C) \mid (- \ C) \mid (- \ v \ C) \mid (Abs \ C) \mid (Ite \ C \ e \ e) \mid (= \ C \ e) \mid (= \ v \ C) \mid (< \ C \ e) \mid (< \ v \ C) \mid (Call \ C) \mid (Proj_1 \ C) \mid (Proj_2 \ C) \]

\[ e \mapsto e' \] Expression \( e \) reduces to \( e' \)

\[ (+ \ n_1 n_2) \mapsto_R (n_1 + n_2) \]

\[ (- \ n_1 n_2) \mapsto_R (n_1 - n_2) \]

\[ (Abs \ n) \mapsto_R |n| \]

\[ (= \ n_1 n_2) \mapsto_R (n_1 = n_2) \]

\[ (< \ n_1 n_2) \mapsto_R (n_1 < n_2) \]

\[ (Ite \ True \ e_1 \ e_2) \mapsto_R e_1 \]

\[ (Ite \ True \ e_1 \ e_2) \mapsto_R e_1 \]

\[ (Call \ (Lam \ x \ S \ e) \ v) \mapsto_R [v/x] e \]

\[ (Proj_1 \ (Pair \ v_1 \ v_2)) \mapsto_R v_1 \]

\[ (Proj_2 \ (Pair \ v_1 \ v_2)) \mapsto_R v_2 \]

\[ (Split \ (Pair \ v_1 \ v_2) \ (x_1 x_2 => e_12)) \mapsto_R [v_1/x_1][v_2/x_2]e_12 \]

\[ (Rec \ f \ S \ e) \mapsto_R [(Rec \ f \ S \ e) / f] e \]

\[ e \mapsto e' \] expression \( e \) takes one step to \( e' \)

\[ \text{step-context} \]

\[ C[e] \mapsto C[e'] \]
§3 Progress

Question 3(a). Progress says that

If $\emptyset \vdash e : S$ then either (1) $e$ is a value, or (2) there exists $e'$ such that $e \rightarrow e'$.

For most languages, including ours, it is impossible to prove progress without first proving a lemma known as canonical forms or value inversion.

The first name, canonical forms, comes from the idea that the values of a given type—as opposed to expressions that are not values—are the original or canonical forms of that type. For example, while $(+ 1 1)$ and $(- 5 3)$ and $(- (\text{Abs} -3) 1)$ are all expressions of type int—and, in a sense, represent the same integer 2 since they all eventually step to 2—we would not consider these expressions as defining the set of integers. But we can say that the values of type int—which are the integer constants $n$—define the integers.

The second name, value inversion, comes from the fact that the lemma uses inversion on a given derivation—but not the inversion we have often used, where we reason either from (a) knowing that we have an expression $e$ of a particular form, say $\text{Call } e_1 e_2$, or (b) knowing that the conclusion of a derivation is by some particular rule, say $\rightarrow \text{Elim}$. Instead, the inversion is based on the combination of two facts:

- We know that the expression is a value.
- We know something about the expression’s type.

Here is the complete value inversion, or canonical forms, lemma for our current language. There is one part for each production in the grammar of types.

Lemma 1 (Value Inversion).

1. If $\emptyset \vdash v : \text{unit}$ then $v = ()$.
2. If $\emptyset \vdash v : \text{bool}$ then either $v = \text{True}$ or $v = \text{False}$.
3. If $\emptyset \vdash v : \text{int}$ then there exists $n$ such that $v = n$.
4. If $\emptyset \vdash v : (S_1 \times S_2)$ then there exist $v_1$ and $v_2$ such that $v = (\text{Pair } v_1 v_2)$ and $\emptyset \vdash v_1 : S_1$ and $\emptyset \vdash v_2 : S_2$.
5. If $\emptyset \vdash v : (S_1 \rightarrow S_2)$ then there exist $x$ and $e$ such that $v = (\text{Lam } x S_1 e)$ and $x : S_1 \vdash e : S_2$.

Proof. [Unusually, this proof does not need induction.]

Part 1: The only rule whose conclusion can be $\emptyset \vdash ()$ is unitIntro. By inversion on unitIntro, we have $v = ()$. [In full detail for the impossible cases:

- In type-assum, we have $x$ (which is a value) but the context is $\emptyset$, so the premise is $(x : \text{unit}) \in \emptyset$ which is impossible.
- In $\rightarrow \text{Intro}$, the expression being typed is a value, but the type is a $\rightarrow$ which does not match the given unit, so this case is impossible.
- In $\rightarrow \text{Elim}$, the expression being typed has the form $\text{Call } e_1 e_2$, which is not a value.
- In type-true, type-false and intIntro, the expression being typed is a value but the type does not match.
§3 Progress

- In type-add, type-sub, type-abs, type-equals, type-lt, type-ite, ×Elim1, ×Elim2, type-split and type-rec, the expression being typed is not a value.

- In ×Intro, the expression being typed could be a value (if the two subexpressions \(e_1\) and \(e_2\) are values, then \((\text{Pair } e_1 e_2)\) is a value), but the type does not match.

End of the detail for the impossible cases.

Part 2: [proof omitted]
Part 3: [proof omitted]
Part 4: **Question 3(a).** Fill in the four listed cases.
Consider cases of the rule concluding \(\emptyset \vdash v : (S_1 \times S_2)\). [Either explain why the case is impossible, even if you are only repeating what I gave for Part 1, or show the goal for Part 4 as stated by the lemma.]

- type-assum:
  In type-assum, we have \(x\) (which is a value) but the context is \(\emptyset\), so the premise is \((x : S_1 \times S_2) \in \emptyset\) which is impossible.

- →Intro:
  By inversion on →Intro, \((S_1 \times S_2) = (T_1 \rightarrow T_2)\) which is impossible.

- ×Elim: [There is no rule with this name! I should have picked either ×Elim1 or ×Elim2.]
  By inversion on ×Elim1, \(v = \text{proj}_1 e\) which is impossible: a Proj is never a value, according to the grammar of values.

- ×Intro:
  [This is the only possible case. There is no need to explain why the case is possible: our “starting position” is that every case is possible. If a case is impossible, explain why; otherwise, do the case, which means: “show the goal for Part 4 as stated by the lemma”.

  [Our goal is the goal for Part 4, namely: “there exist \(v_1\) and \(v_2\) such that \(v = (\text{Pair } v_1 v_2)\) and \(\emptyset \vdash v_1 : S_1\) and \(\emptyset \vdash v_2 : S_2\)”.]

  \(v = (\text{Pair } v_1 v_2)\) By inversion on rule ×Intro
  \(\emptyset \vdash v_1 : S_1\) "
  \(\emptyset \vdash v_2 : S_2\) "

  [These are exactly the three goals we need, so we're done! A longer, equally valid proof would be:]

  \(v = (\text{Pair } e_1 e_2)\) By inversion on rule ×Intro
  \(\emptyset \vdash v_1 : S_1\) "
  \(\emptyset \vdash v_2 : S_2\) "
  \(e_1\) is a value, that is, \(e_1 = v_1\) By the grammar of values
  \(e_2\) is a value, that is, \(e_2 = v_2\) By the grammar of values
  \(v = (\text{Pair } v_1 v_2)\) By above equations

- The remaining cases are impossible for reasons similar to those given in Part 1.
§3 Progress

Part 5: Question 3(b). Complete the missing case.

• \( \to \text{Intro} \):
  \[ v = (\text{Lam } x S_1 e) \quad \text{By inversion on rule } \to \text{Intro} \]
  \[ x : S_1 \vdash e : S_2 \quad " \]

[These are exactly the two things we need for Part 5, so we’re done.]

• The remaining cases are impossible for reasons similar to those given in Part 1.

Question 3(c)+. For the type \( \bot \) (see Question 2), value inversion is a little unusual. State and prove the appropriate lemma.

The high-level idea is that the lemma should say that it is impossible for a value to have type \( \bot \). There are several different correct ways to phrase this, including:

• “It is not the case that \( \emptyset \vdash v : \bot \).”
• “There does not exist a value \( v \) such that \( \emptyset \vdash v : \bot \).”
• “There does not exist an expression \( e \) such that \( \emptyset \vdash e : \bot \) and \( e \) is not a value.”
• “For all \( v \), if \( \emptyset \vdash v : \bot \) then we have a contradiction.”
• “For all \( v \), if \( \emptyset \vdash v : \bot \) then impossible.”

Some mathematicians would probably object to the last one, on the grounds that “then impossible” is not a valid statement. I don’t object to it, because I would read “impossible” as “we have a contradiction”, which I think most mathematicians would tolerate. I especially like the last one, because the shape of the statement looks just like the other statements of value inversion: “For all \( v \), if \( \emptyset \vdash v : \text{some type connective} \) then something.”

The proof (of any of the above statements) looks similar to the other parts of value inversion: a great many cases are impossible. The difference is that all of the cases are impossible.

Some other phrasings that say almost the same thing (and could be used in the same way) include:

• “If \( \emptyset \vdash e : \bot \) then \( e \) is not a value.”
• “If \( \emptyset \vdash v : S \) then \( S \neq \bot \).”

For the first of these two, the proof would look slightly different: several cases are possible, including \( \to \text{Elim}, \times \text{Elim1}, \times \text{Elim2}, \text{type-split} \) and \( \text{type-rec} \); but in all of those rules, we find by inversion that the expression \( e \) is not a value, which is our goal.

For the second, the set of possible cases is different but the structure of the possible cases is similar: for example, the case \( \times \text{Intro} \) is possible but we find by inversion that \( S = S_1 \times S_2 \), which is not equal to \( \bot \).