

Homework # 8

due October 28

1 Reading

Please read Chapter 13 in your textbook.

2 Problems

Please do the following problem:

- Exercise 13.1.1, and include the effects of evaluating

```
c = (lambda x: Nat . {ref x, ref x}) 0
```

Explain your answer!

3 Discussion

The textbook says (page 167) that we must include a well typing in the requirements for progress and preservation. Give two counter-examples, one for Progress (Theorem 13.5.7) and one for Preservation (Theorem 13.5.3) if they omit any mention of well typing.

4 Proofs

Put together the proof of progress. The solution uses the following three “effectiveness” lemmas:

- Given a particular term and memory, it is always possible to allocate a cell for it.
- If we have a well-typed memory, and the memory typing has a binding for a location, then so does the memory typing. That is, if $* \mid \Sigma \vdash \mu$ and $\Sigma(l) = T$, then there exists a term t such that $\mu(l) = t$. (That it has the right type is part of preservation, not progress.)
- If we have a well-typed memory and the memory typing has a binding for a location, then we can update the memory at that location.

These three lemmas do the work of progress for allocation, dereference and assignment, respectively.

5 Extra

Optionally, complete the proof of preservation of references started in the SASyLF skeleton file.

6 Graduate Students

The model in the textbook doesn't handle pointer arithmetic. Find and cite published proofs of soundness of systems with pointer arithmetic. How does the model change? What new types are needed? Are there any mechanized proofs?