Haskell Concurrency and STM

Johannes Åman Pohjola
UNSW
Term 3 2022
Shared Data

Consider the **Readers and Writers** problem:

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>We have a <strong>large shared data structure</strong>, that can’t be updated in one atomic step. <strong>Writers</strong> are updating it, and <strong>readers</strong> try to retrieve a coherent copy of it.</td>
</tr>
</tbody>
</table>

We want:

- **Atomicity**: partial updates are not observable.
- **Consistency**: any reader that starts after a finished update will see that update.
- Minimal **waiting**.
A Crappy Solution

Treat both reads and updates as critical sections — use any old critical section solution (locks, etc.) to sequentialise all reads and writes.

Observation

Updates are *atomic* and reads are *consistent*—but reads can’t happen concurrently, which leads to unnecessary *contention*. 
A Better Solution

A more elaborate locking mechanism (condition variables) could be used to allow multiple concurrent readers. Writers still require exclusive access.

**Observation**

This reduces contention. We can’t let updates execute concurrently with reads; otherwise, partial updates would be observable.
Complication

Suppose we don’t want readers to wait (much) while an update is performed. Instead, we’ll give them an older version of the data.

**Trick:** A writer creates *their own local copy* of the data, and then updates just the *pointer* to the data.

- **Atomicity**  The only shared write is now just to one pointer.
- **Consistency**  Reads that start before the pointer update get the older version, but reads that start after get the latest.
Persistent Data Structures

Copying is $O(n)$ in the worst case, but we can do better for many tree-like structures.

Example (Binary Search Tree)
Purely Functional Data Structures

Persistent data structures that use of copying (rather than mutation) are called *purely functional* data structures. Operations on them can be expressed as mathematical functions that, given an input structure, return a *new* output structure:

\[
\begin{align*}
\text{insert } v \text{ Leaf} &= \text{Branch } v \text{ Leaf Leaf} \\
\text{insert } v (\text{Branch } x \text{ l r}) &= \text{if } v \leq x \text{ then} \\
& \quad \text{Branch } x (\text{insert } v \text{ l}) \text{ r} \\
& \text{else} \\
& \quad \text{Branch } x \text{ l (insert } v \text{ r)}
\end{align*}
\]
Computing with Functions

We model processes in Haskell using the \texttt{IO} type. We’ll treat \texttt{IO} as an abstract type for now, and give it a formal semantics later if we have time:

\[
\text{IO } \tau = \text{A (possibly effectful) process that, when executed, produces a result of type } \tau
\]

Note the semantics of \textit{evaluation} and \textit{execution} are different things.
Building up IO

Recall monads:

\[ \text{return} :: \forall a. \ a \rightarrow \text{IO} \ a \]
\[ (\gg=) :: \forall a \ b. \ \text{IO} \ a \rightarrow (a \rightarrow \text{IO} \ b) \rightarrow \text{IO} \ b \]
\[ \text{getChar} :: \text{IO} \ \text{Char} \]
\[ \text{putChar} :: \text{Char} \rightarrow \text{IO} \ () \]

Example (Echo)

\[ \text{echo} :: \text{IO} \ () \]
\[ \text{echo} = \text{getChar} \gg= (\lambda x. \ \text{putChar} \ x \gg= \lambda y. \ \text{echo}) \]

Or, with do notation:

\[ \text{echo} :: \text{IO} \ () \]
\[ \text{echo} \ = \ \text{do} \ x \leftarrow \text{getChar} \]
\[ \quad \ 	ext{putChar} \ x \]
\[ \quad \text{echo} \]
Adding Concurrency

We can have multiple threads easily enough:

\[ \text{forkIO} :: \text{IO} () \rightarrow \text{IO} () \]

Example (Dueling Printers)

\[
\text{let } \text{loop } \text{c} = \text{do } \text{putChar } \text{c}; \text{loop } \text{c} \\
\text{in } \text{do } \text{forkIO } (\text{loop } \text{`a'}); \text{loop } \text{`z'}
\]

But what sort of \textit{synchronisation primitives} are available?
The **MVar** is the simplest synchronisation primitive in Haskell. It can be thought of as a shared box which holds at most one value.

Processes must take the value out of a **full** box to read it, and must put a value into an **empty** box to update it.

**MVar Functions**

```haskell
newMVar :: ∀a. a → IO (MVar a)  -- Create a new MVar
takeMVar :: ∀a. MVar a → IO a   -- Read/remove the value
putMVar :: ∀a. MVar a → a → IO () -- Update/insert a value
```

Taking from an empty MVar or putting into a full one results in blocking.
An MVar can be thought of as channel containing at most one value.
Readers and Writers

We can treat MVars as shared variables with some definitions:

\[
\begin{align*}
\text{writeMVar } m \ v &= \textbf{do} \ \text{takeMVar } m; \ \text{putMVar } m \ v \\
\text{readMVar } m &= \textbf{do} \ v \leftarrow \text{takeMVar } m; \ \text{putMVar } m \ v; \ \text{return } v
\end{align*}
\]

\[
\text{problem :: } \mathit{DB} \to \mathit{IO} ()
\]

\[
\text{problem initial = do}
\]

\[
\begin{align*}
\text{db} &\leftarrow \text{newMVar } \text{initial} \\
\text{wl} &\leftarrow \text{newMVar } () \\
\textbf{let} \ \text{reader} = \text{readMVar } db \\
\textbf{let} \ \text{writer} = \textbf{do} \\
\text{takeMVar } \text{wl} \\
\text{d} &\leftarrow \text{readMVar } db \\
\textbf{let} \ d' = \text{update } d \\
\text{evaluate } d' \\
\text{writeMVar } db \ d' \\
\text{putMVar } \text{wl } ()
\end{align*}
\]
Fairness

Each MVar has an attached FIFO queue, so GHC Haskell can ensure the following fairness property:

*No thread can be blocked indefinitely on an MVar unless another thread holds that MVar indefinitely.*
The Problem with Locks

**Problem**

Write a procedure to transfer money from one bank account to another. To keep things simple, both accounts are held in memory: no interaction with databases is required. The procedure must operate correctly in a concurrent program, in which many threads may call transfer simultaneously. No thread should be able to observe a state in which the money has left one account, but not arrived in the other (or vice versa).
The Problem with Locks

Assume some infrastructure for accounts:

\[
\begin{align*}
\textbf{type} & \quad \text{Balance} = \text{Int} \\
\textbf{type} & \quad \text{Account} = \text{MVar} \ \text{Balance} \\

\textit{withdraw} & \quad :: \quad \text{Account} \rightarrow \text{Int} \rightarrow \text{IO} () \\
\textit{withdraw} & \quad a \ m = \text{takeMVar} \ a \ \gg (\text{putMVar} \ a \ \circ \ \text{subtract} \ m) \\

\textit{deposit} & \quad :: \quad \text{Account} \rightarrow \text{Int} \rightarrow \text{IO} () \\
\textit{deposit} & \quad a \ m = \text{withdraw} \ a \ (-m)
\end{align*}
\]
Attempt #1

\[
\text{transfer } f \ t \ m = \textbf{do} \ \text{withdraw } f \ m; \text{deposit } t \ m
\]

Problem

The intermediate states where a transaction has only been partially completed are externally observable.

In a bank, we might want the invariant that at all points during the transfer, the total amount of money in the system remains constant. We should have no money go missing.
Attempt #2

```
transfer f t m = do
  fb ← takeMVar f
  tb ← takeMVar t
  putMVar t (tb + m)
  putMVar f (fb - m)
```

Problem

We can have *deadlock* here, when two people transfer to each other simultaneously and both transfers proceed in lock-step.

Also, we can’t just compose our existing *withdrawal* and *deposit* operations. That’s sad.
Solution

We should enforce a *global* ordering of locks.

```haskell
type Account = (MVar Balance, AccountNo)

transfer (f, fa) (t, ta) m = do
  (fb, tb) ← if fa ≤ ta
    then do
      fb ← takeMVar f
      tb ← takeMVar t
      pure (fb, tb)
    else do
      tb ← takeMVar t
      fb ← takeMVar f
      pure (fb, tb)
  putMVar t (tb + m)
  putMVar f (fb - m)
```
Problem

Now suppose that some accounts can be configured with a “backup” account, that is used if insufficient funds are available in the default account.

Should you take the lock for the backup account?

To make life even harder: What if we want to block if insufficient funds are available?
Conclusion

*Lock-based methods* have their place, but from a software engineering perspective they’re a nightmare.

- Remember not to take too many locks.
- Remember not to take too few locks.
- Remember what locks correspond to each piece of shared data.
- Remember not to take the locks in the wrong order.
- Remember to deal with locks when an error occurs.
- Remember to signal condition variables and release locks at the right time.

Most importantly, *modular programming* becomes impossible.
The Solution

Represent an account as a simple shared variable containing the balance.

\[
\text{transfer } f \ t \ m = \text{atomically } \$ \ do
\]
\[
\text{withdraw } f \ m
\]
\[
\text{deposit } t \ m
\]

Where \textit{atomically } \( P \) guarantees:

\textbf{Atomicity} The effects of the action \( P \) become visible all at once.

\textbf{Isolation} The effects of action \( P \) is not affected by any other threads.

**Problem**

How can we implement \textit{atomically}?
We can adopt the solution of certain reptilian programming languages.

**Problem**

Atomicity is guaranteed, but what about *isolation*?
Also, performance is predictably garbage.
Ensuring Isolation

Rather than use regular shared variables, use special *transactional variables*.

\[
\begin{align*}
\text{newTVar} & \quad :: \quad a \rightarrow \text{STM} \ (\text{TVar} \ a) \\
\text{readTVar} & \quad :: \quad \text{TVar} \ a \rightarrow \text{STM} \ a \\
\text{writeTVar} & \quad :: \quad \text{TVar} \ a \rightarrow a \rightarrow \text{STM} \ ()
\end{align*}
\]

\[
\begin{align*}
\text{atomically} & \quad :: \quad \text{STM} \ a \rightarrow \text{IO} \ a
\end{align*}
\]

The type constructor \text{STM} is also an instance of the *Monad* type class, and thus supports the same basic operations as \text{IO}.

\[
\begin{align*}
\text{pure} & \quad :: \quad a \rightarrow \text{STM} \ (\text{TVar} \ a) \\
(\gg=) & \quad :: \quad \text{STM} \ a \rightarrow (a \rightarrow \text{STM} \ b) \rightarrow \text{STM} \ b
\end{align*}
\]
**Implementing Accounts**

\[
\text{type Account} = \text{TVar Int}
\]

\[
\text{withdraw} :: \text{Account} \rightarrow \text{Int} \rightarrow \text{STM} ()
\]

\[
\text{withdraw a m} = \text{do}
\]

\[
\text{balance} \leftarrow \text{readTVar m}
\]

\[
\text{writeTVar a (balance} - m)
\]

\[
\text{deposit a m} = \text{withdraw a (m)}
\]

**Observe:** \text{withdraw} (resp. \text{deposit}) can only be called inside an atomically ⇒ We have isolation.

But, we’d still like to run more than one transaction at once — one global lock isn’t good enough.
Optimistic Execution

Each transaction (atomically block) is executed *optimistically*. This means they do not need to check that they are allowed to execute the transaction first (unlike, say, locks, which prefer a *pessimistic* model).

**Implementation Strategy**

Each transaction has an associated *log*, which contains:

- The values written to any *TVars* with *writeTVar*.
- The values read from any *TVars* with *readTVar*, consulting earlier log entries first.

First the log is *validated*, and, if validation succeeds, changes are *committed*. Validation and commit are one atomic step.

What can we do if validation fails? We re-run the transaction!
Re-running transactions

```haskell
atomically $ do
  x ← readTVar xv
  y ← readTVar yv
  if x > y then detonateTNT else pure ()
```

To avoid harmful side-effects, the transaction must be *repeatable*. We can’t change the world until *commit* time.

A real implementation is smart enough not to retry with exactly the same schedule.
Blocking and *retry*

**Problem**

We want to *block* if insufficient funds are available.

We can use the helpful action `retry :: STM a`.

```hs
withdraw' :: Account -> Int -> STM ()
withdraw' a m = do
  balance ← readTVar a
  if m > 0 && m > balance then
    retry
  else
    writeTVar a (balance - m)
```
Choice and *orElse*

**Problem**

We want to transfer from a backup account if the first account has insufficient funds, and *block* if neither account has insufficient funds.

We can use the helpful action

\[
\text{orElse} :: \text{STM } a \rightarrow \text{STM } a \rightarrow \text{STM } a
\]

\[
\text{wdBackup} :: \text{Account } \rightarrow \text{Account } \rightarrow \text{Int } \rightarrow \text{STM } ()
\]

\[
\text{wdBackup } a_1 \ a_2 \ m = \text{orElse } (\text{withdraw'} \ a_1 \ m) \ (\text{withdraw'} \ a_2 \ m)
\]
Evaluating STM

STM is *modular*. We can compose transactions out of smaller transactions. We can hide concurrency behind library boundaries without worrying about deadlock or global invariants.

Lock-free data structures and transactional memory based solutions work well if contention is low and under those circumstances scale better to higher process numbers than lock-based ones.

Most importantly, the resulting code is often simpler and more robust. **Profit!**
Progress

One transaction can force another to abort only when it commits.

At any time, at least one currently running transaction can successfully commit.

Traditional deadlock scenarios are impossible, as is cyclic restarting where two transactions constantly cancel each other.

Starvation is possible (when?), however uncommon in practice. So, we technically don’t have eventual entry.
Database Guarantees

Atomicity ✓ Each transaction should be ‘all or nothing’.

Consistency ✓ Each transaction in the future sees the effects of transactions in the past.

Isolation ✓ The transaction’s effect on the state cannot be affected by other transactions.

Durability The transaction’s effect on the state survives power outages and crashes.

STM gives you 75% of a database system. The Haskell package acid-state builds on STM to give you all four.
That’s it

We have now covered all the content in COMP3161/COMP9164. Thanks for sticking with the course.

- **Syntax Foundations**
  Concrete/Abstract Syntax, Ambiguity, HOAS, Binding, Variables, Substitution, $\lambda$-calculus

- **Semantics Foundations**
  Static Semantics, Dynamic Semantics (Small-Step/Big-Step), Abstract Machines, Environments, Stacks, Safety, Liveness, Type Safety (Progress and Preservation)

- **Features**
  - Algebraic Data Types, Recursive Types
  - Exceptions
  - Polymorphism, Type Inference, Unification
  - Overloading, Subtyping, Abstract Data Types
  - Concurrency, Critical Sections, STM
MyExperience

Please fill out the survey. It helps tremendously.

https://myexperience.unsw.edu.au
Further Learning

- UNSW courses:
  - COMP3141 — Software System Design and Implementation
  - COMP6721 — (In-)formal Methods
  - COMP3131 — Compilers
  - COMP4141 — Theory of Computation
  - COMP3151 — Foundations of Concurrency
  - COMP4161 — Advanced Topics in Verification
  - COMP3153 — Algorithmic Verification

- Online Learning
  - Oregon Programming Languages Summer School Lectures
    ([https://www.cs.uoregon.edu/research/summerschool/archives.html](https://www.cs.uoregon.edu/research/summerschool/archives.html)) Videos are available from here! Also some on YouTube.
What’s next?

The exam is on **Monday, 5th of December 2022** at 9am.

- I have posted a sample exam with revision questions.
- The final exam will run similar to the sample exam.
- It runs for 2 hours and 10 minutes.
Evaluation Semantics

The semantics of Haskell’s evaluation are interesting but not particularly relevant for us. We will assume that it happens quietly without a fuss:

\[
\begin{align*}
\beta\text{-equivalence} \quad & (\lambda x. M[x]) \ N \equiv_{\beta} M[N] \\
\alpha\text{-equivalence} \quad & \lambda x. M[x] \equiv_{\alpha} \lambda y. M[y] \\
\eta\text{-equivalence} \quad & \lambda x. M \ x \equiv_{\eta} M
\end{align*}
\]

Let our ambient congruence relation \(\equiv\) be \(\equiv_{\alpha\beta\eta}\) enriched with the following extra equations, justified by the monad laws:

\[
\begin{align*}
\text{return } N \gg= M \equiv M \ N \\
(X \gg= Y) \gg= Z \equiv X \gg= (\lambda x. Y \ x \gg= Z) \\
X \equiv X \gg= \text{return}
\end{align*}
\]
Processes

This means that a Haskell expression of type \( \text{IO} \ \tau \) for will boil down to either \( \text{return} \ x \) where \( x \) is a value of type \( \tau \); or \( a \gg M \) where \( a \) is some primitive IO action (\( \text{forkIO} \ p \), \( \text{readMVar} \ v \), etc.) and \( M \) is some function producing another IO \( \tau \). This is the head normal form for IO expressions.

**Definition**

Define a language of processes \( P \), which contains all (head-normal) expressions of type \( \text{IO} () \).

We want to define the semantics of the execution of these processes. Let’s use operational semantics:

\[
(\rightarrow) \subseteq P \times P
\]
Semantics for forkIO

To model forkIO, we need to model the parallel execution of multiple processes in our process language. We shall add a parallel composition operator to the language of processes:

\[
P, Q ::= a \gg M \\
\mid \text{return } () \\
\mid P \parallel Q \\
\mid \ldots
\]

And the following ambient congruence equations:

\[
P \parallel Q \equiv Q \parallel P \\
P \parallel (Q \parallel R) \equiv (P \parallel Q) \parallel R
\]
Semantics for forkIO

If we have multiple processes active, pick one of them non-deterministically to move:

\[ P \leftrightarrow P' \]

\[ P \parallel Q \leftrightarrow P' \parallel Q \]

The \textit{forkIO} operation introduces a new process:

\[ (\text{forkIO } P \gg= M) \leftrightarrow P \parallel (\text{return } () \gg= M) \]
Semantics for MVars

MVars are modelled as a special type of process, identified by a unique name. Values of MVar type merely contain the name of the process, so that putMVar and friends know where to look.

\[
P, Q ::= a \gg M \\
| \quad \text{return } () \\
| \quad P \parallel Q \\
| \quad \langle \rangle_n \mid \langle v \rangle_n \\
| \quad \ldots
\]

\[
\langle \rangle_n \parallel (\text{putMVar } n \; v \gg M) \mapsto \langle v \rangle_n \parallel (\text{return } () \gg M)
\]

\[
\langle v \rangle_n \parallel (\text{takeMVar } n \gg M) \mapsto \langle \rangle_n \parallel (\text{return } \; v \gg M)
\]
Semantics for newMVar

We might think that \( \text{newMVar} \) should have semantics like this:

\[
\left( \text{newMVar } v \gg M \right) \leftrightarrow \langle v \rangle_n \parallel \left( \text{return } n \gg M \right) \text{ (} n \text{ fresh)}
\]

But this approach has a number of problems:

- The name \( n \) is now globally-scoped, without an explicit binder to introduce it.
- It doesn’t accurately model the \textit{lifetime} of the MVar, which should be garbage-collected once all processes that can access it finish.
- It makes MVars \textit{global} objects, so our semantics aren’t very \textit{abstract}. We would like local communication to be local in our model.
Restriction Operator

We introduce a restriction operator $\nu$ to our language of processes:

$$ P, Q ::= a \gg M \mid \text{return } () \mid P \parallel Q \mid \langle \rangle_n \mid \langle v \rangle_n \mid (\nu \; n) \; P $$

Writing $(\nu \; n) \; P$ says that the MVar name $n$ is only available in process $P$. Mentioning $n$ outside $P$ is not well-formed. We need the following additional congruence equations:

$$ (\nu \; n) \; (\nu \; m) \; P \equiv (\nu \; m) \; (\nu \; n) \; P $$
$$ (\nu \; n)(P \parallel Q) \equiv P \parallel (\nu \; n) \; Q \quad \text{(if } n \notin P \text{)} $$
Better Semantics for newMVar

The rule for \textit{newMVar} is much the same as before, but now we explicitly restrict the MVar to \( M \).

\[
\begin{align*}
(newMVar \ v \gg M) & \leftrightarrow (\nu \ n)(\langle v \rangle_n \parallel (\text{return } n \gg M)) (n \text{ fresh})
\end{align*}
\]

We can always execute under a restriction:

\[
\begin{align*}
P & \leftrightarrow P' \\
(\nu \ n) P & \leftrightarrow (\nu \ n) P'
\end{align*}
\]

Question

What happens when you put an MVar inside another MVar?
Garbage Collection

If an MVar is no longer used, we just replace it with the do-nothing process:

\[
(\nu \ n) \langle \rangle_n \ \overset{\leftrightarrow}{\mapsto} \ \text{return} ()
\]

\[
(\nu \ n) \langle v \rangle_n \ \overset{\leftrightarrow}{\mapsto} \ \text{return} ()
\]

Extra processes that have outlived their usefulness disappear:

\[
\text{return} () \parallel P \ \overset{\leftrightarrow}{\mapsto} \ P
\]
Our language $P$ is called a \textit{process algebra}, a common means of describing semantics for concurrent programs.
Bibliography

Simon Marlow
Parallel and Concurrent Programming in Haskell
O'Reilly, 2013
http://chimera.labs.oreilly.com/books/1230000000929

Simon Peyton Jones, Andrew Gordon and Sigbjorn Finne
Concurrent Haskell
POPL ’96
Association for Computer Machinery

Simon Marlow (Editor)
Haskell 2010 Language Report
https://www.haskell.org/onlinereport/haskell2010/
Bibliography

Simon Peyton Jones
Beautiful Concurrency

Tim Harris, Simon Marlow, Simon Peyton Jones, Maurice Herlihy
Composable Memory Transactions
PPoP ’05
Association for Computer Machinery

David Himmelstrup
Acid-State Library
https://github.com/acid-state/acid-state

Ryan Yates and Michael L. Scott
A Hybrid TM for Haskell
TRANSACT ’14
Association for Computer Machinery