MODULE *MapCache*

EXTENDS *Naturals*, *FiniteSets*, *Sequences*, *TLC*

An empty value
CONSTANT *Nil*

The set of clients to model
CONSTANT *Client*

The set of possible keys in the map
CONSTANT *Key*

The set of possible values in the map
CONSTANT *Value*

An update entry identifier
CONSTANT *Update*

A tombstone entry identifier
CONSTANT *Tombstone*

The system state, modelled as a strongly consistent consensus service
using a single mapping of $key \to value$ pairs
VARIABLE *state*

A sequential version number, used by the consensus service to assign logical
timestamps to entries
VARIABLE *stateVersion*

The cache state
VARIABLE *cache*

The maximum version propagated to the cache
VARIABLE *cacheVersion*

An unordered bag of pending cache entries
VARIABLE *cachePending*

A strongly ordered sequence of update events
VARIABLE *events*

The history of history for the client, used by the model checker to verify sequential consistency
VARIABLE *history*

$vars \triangleq \langle state, stateVersion, cache, cachePending, cacheVersion, events, history \rangle$

The type invariant checks that the client's history never go back in time

$$
\begin{array}{l}
\mathit{TypeInvariant} \triangleq \\
\quad \land \forall\, c \in \mathit{Client} : \\
\qquad \land \forall\, k \in \mathit{Key} : \\
\qquad\quad \land \forall\, r \in \text{DOMAIN } \mathit{history}[c][k] : \\
\qquad\qquad r > 1 \Rightarrow \mathit{history}[c][k][r] \geq \mathit{history}[c][k][r-1]
\end{array}
$$

This section models helpers for managing the system and cache state

Drop a key from the domain of a function

$$\mathit{DropKey}(s,\, k) \triangleq [i \in \text{DOMAIN } s \setminus \{k\} \mapsto s[i]]$$

Put an entry in the given function

$$
\begin{array}{l}
\mathit{PutEntry}(s,\, e) \triangleq \\
\quad \text{IF } e.\mathit{key} \in \text{DOMAIN } s \text{ THEN} \\
\qquad [s \text{ EXCEPT } ![e.\mathit{key}] = e] \\
\quad \text{ELSE} \\
\qquad s \mathbin{@@} (e.\mathit{key} :> e)
\end{array}
$$

This section models the map cache. When a client updates the map, it defers updates to the cache to be performed in a separate step. The cache also listens for events coming from a consensus service, which must provide sequentially consistent event streams. Entries are arbitrarily evicted from the cache.

Defer an entry 'e' to be cached asynchronously on client 'c'
Updates are deferred in no particular order to model the potential reordering of
concurrent thhistory by the operating system.

$$
\begin{array}{l}
\mathit{DeferCache}(c,\, e) \triangleq \\
\quad \mathit{cachePending}' = [\mathit{cachePending} \text{ EXCEPT } ![c] = \mathit{cachePending}[c] \mathbin{@@} (e.\mathit{version} :> e)]
\end{array}
$$

Remove a deferred entry 'e' from cache deferrals for client 'c'

$$
\begin{array}{l}
\mathit{RemoveCacheDeferral}(c,\, e) \triangleq \\
\quad \mathit{cachePending}' = [\mathit{cachePending} \text{ EXCEPT } ![c] = \\
\qquad [v \in \text{DOMAIN } \mathit{cachePending}[c] \setminus \{e.\mathit{version}\} \mapsto \mathit{cachePending}[c][v]]]
\end{array}
$$

Cache an entry 'e' on client 'c'
The entry is read from the pending cache entries. An entry will only be updated
in the cache if the entry version is greater than the cache propagation version,
ensuring the cache cannot go back in time.
Note that removals are inserted into the cache as tombstones to be removed once
updates have been propagated via event queues.

$$
\begin{array}{l}
\mathit{Cache}(c,\, e) \triangleq \\
\quad \land \text{LET } \mathit{entry} \triangleq \mathit{cachePending}[c][e] \\
\qquad \text{IN} \\
\qquad\quad \land \lor \land \mathit{entry.version} > \mathit{cacheVersion}[c] \\
\qquad\qquad\quad \land \lor \mathit{entry.key} \notin \text{DOMAIN } \mathit{cache}[c]
\end{array}
$$

```
                    ∨ ∧ entry.key ∈ DOMAIN cache[c]
                      ∧ entry.version > cache[c][entry.key].version
                  ∧ cache' = [cache EXCEPT ![c] = PutEntry(cache[c], entry)]
                  ∧ history' = [history EXCEPT ![c][entry.key] =
                      Append(history[c][entry.key], entry.version)]
              ∨ ∧ ∨ entry.version ≤ cacheVersion[c]
                    ∨ ∧ entry.key ∈ DOMAIN cache[c]
                      ∧ entry.version ≤ cache[c][entry.key].version
                  ∧ UNCHANGED ⟨cache, history⟩
          ∧ RemoveCacheDeferral(c, entry)
    ∧ UNCHANGED ⟨state, stateVersion, cacheVersion, events⟩
```

Enqueue a cache update event 'e' for all clients
Events are guaranteed to be delivered to clients in the order in which they
occurred in the consensus layer, so we model events as a simple strongly ordered
sequence.

```
EnqueueEvent(e) ≜
    events' = [i ∈ Client ↦ Append(events[i], e)]
```

Learn a map update from the event queue of 'c'
The learner learns the first entry in the event queue for client 'c'.
If the key is already in the cache, the learner updates the key only if
the update version is at least as great as the cached version.
If the key is not present in the map, the entry is cached.
Tombstone types are removed from the cache. Entry types are inserted.
Once caching is complete, the 'cacheVersion' is updated to ensure the
deferred cache remains consistent.

```
Learn(c) ≜
    ∧ Cardinality(DOMAIN events[c]) > 0
    ∧ LET entry ≜ events[c][1]
      IN
          ∧ ∨ ∧ entry.key ∈ DOMAIN cache[c]
              ∧ entry.version ≥ cache[c][entry.key].version
              ∧ ∨ ∧ entry.type = Update
                  ∧ cache' = [cache EXCEPT ![c] = PutEntry(cache[c], entry)]
                ∨ ∧ entry.type = Tombstone
                  ∧ cache' = [cache EXCEPT ![c] = DropKey(cache[c], entry.key)]
            ∨ ∧ ∨ entry.key ∉ DOMAIN cache[c]
                ∨ ∧ entry.key ∈ DOMAIN cache[c]
                  ∧ entry.version < cache[c][entry.key].version
              ∧ UNCHANGED ⟨cache⟩
          ∧ cacheVersion' = [cacheVersion EXCEPT ![c] = entry.version]
    ∧ events' = [events EXCEPT ![c] = SubSeq(events[c], 2, Len(events[c]))]
    ∧ UNCHANGED ⟨state, stateVersion, cachePending, history⟩
```

Evict a map key 'k' from the cache of client 'c'

To preserve consistency, each key for each client must be retained until updates prior to the key version have been propagated to the client. If keys are evicted before updates have been propagated to the cache, evicting a key can allow a concurrent *Put* or *Remove* to cache an older entry.

$$
\begin{aligned}
&Evict(c,\ k)\ \triangleq \\
&\quad \land\ k \in \text{DOMAIN}\ cache[c] \\
&\quad \land\ cache[c][k].version \leq cacheVersion[c] \\
&\quad \land\ cache' = [cache\ \text{EXCEPT}\ ![c] = DropKey(cache[c],\ k)] \\
&\quad \land\ \text{UNCHANGED}\ \langle state,\ stateVersion,\ cachePending,\ cacheVersion,\ events,\ history\rangle
\end{aligned}
$$

This section models the method calls for the Map primitive. Map entries can be created, updated, deleted, and read. The *Put* and *Remove* steps model writes to a consensus service. Steps do not atomically cache reads/updates but instead defer them to be cached in a separate step. This models the reordering of threads by the *OS*.

Get an entry for key 'k' in the map on client 'c'
If the key is present in the cache, read from the cache.
If the key is not present in the cache, read from the system state and update the cache if the system entry version is greater than the cache version.
If the key is neither present in the cache or the system state, read the cache version.
If the step reads from the cache, the cached version is added to the history. Otherwise, if the step reads from the consensus service, the cache is updated in a separate step before recording the value.

$$
\begin{aligned}
&Get(c,\ k)\ \triangleq \\
&\quad \land\ \lor\ \land\ k \in \text{DOMAIN}\ cache[c] \\
&\qquad\quad \land\ history' = [history\ \text{EXCEPT}\ ![c][k] = Append(history[c][k],\ cache[c][k].version)] \\
&\qquad\quad \land\ \text{UNCHANGED}\ \langle cachePending\rangle \\
&\qquad \lor\ \land\ k \notin \text{DOMAIN}\ cache[c] \\
&\qquad\quad \land\ k \in \text{DOMAIN}\ state \\
&\qquad\quad \land\ DeferCache(c,\ state[k]) \\
&\qquad\quad \land\ \text{UNCHANGED}\ \langle history\rangle \\
&\qquad \lor\ \land\ k \notin \text{DOMAIN}\ cache[c] \\
&\qquad\quad \land\ k \notin \text{DOMAIN}\ state \\
&\qquad\quad \land\ DeferCache(c,\ [type \mapsto Tombstone, \\
&\qquad\qquad\qquad\qquad key \mapsto k, \\
&\qquad\qquad\qquad\qquad value \mapsto Nil, \\
&\qquad\qquad\qquad\qquad version \mapsto stateVersion]) \\
&\qquad\quad \land\ \text{UNCHANGED}\ \langle history\rangle \\
&\quad \land\ \text{UNCHANGED}\ \langle state,\ stateVersion,\ cache,\ cacheVersion,\ events\rangle
\end{aligned}
$$

Put key 'k' and value 'v' pair in the map on client 'c'
Increment the system state version and insert the entry into the system state.
Enqueue update events to notify all clients and defer a local cache update to client 'c'.

$$
Put(c,\ k,\ v)\ \triangleq
$$

$\land\ stateVersion' = stateVersion + 1$
$\land$ LET $entry \triangleq [type \mapsto Update,\ key \mapsto k,\ value \mapsto v,\ version \mapsto stateVersion']$
IN
$\land\ state' = PutEntry(state,\ entry)$
$\land\ EnqueueEvent(entry)$
$\land\ DeferCache(c,\ entry)$
$\land$ UNCHANGED $\langle cache,\ cacheVersion,\ history\rangle$

Remove key 'k' from the map on client 'c'
Increment the system state version and remove the entry from the system state.
Enqueue tombstone events to notify all clients and defer a local cache update
to client 'c'.

$Remove(c,\ k) \triangleq$
$\land\ k \in$ DOMAIN $state$
$\land\ stateVersion' = stateVersion + 1$
$\land$ LET $entry \triangleq [type \mapsto Tombstone,\ key \mapsto k,\ value \mapsto Nil,\ version \mapsto stateVersion']$
IN
$\land\ state' = DropKey(state,\ k)$
$\land\ EnqueueEvent(entry)$
$\land\ DeferCache(c,\ entry)$
$\land$ UNCHANGED $\langle cache,\ cacheVersion,\ history\rangle$

$Init \triangleq$
$\land$ LET $nilEntry \triangleq [type \mapsto Nil,$
$key \mapsto Nil,$
$value \mapsto Nil,$
$version \mapsto Nil]$
IN
$\land\ state = [i \in \{\} \mapsto nilEntry]$
$\land\ stateVersion = 0$
$\land\ cache = [c \in Client \mapsto [i \in \{\} \mapsto nilEntry]]$
$\land\ cachePending = [c \in Client \mapsto [i \in \{\} \mapsto nilEntry]]$
$\land\ cacheVersion\ = [c \in Client \mapsto 0]$
$\land\ events = [c \in Client \mapsto [i \in \{\} \mapsto nilEntry]]$
$\land\ history = [c \in Client \mapsto [k \in Key \mapsto \langle\rangle]]$

$Next \triangleq$
$\lor \exists\, c \in Client :$
$\exists\, k \in Key :$
$Get(c,\ k)$
$\lor \exists\, c \in Client :$
$\exists\, k \in Key :$
$\exists\, v \in Value :$
$Put(c,\ k,\ v)$

$\lor \exists\, c \in \mathit{Client} :$
$\quad \exists\, k \in \mathit{Key} :$
$\quad\quad \mathit{Remove}(c,\, k)$
$\lor \exists\, c \in \mathit{Client} :$
$\quad \exists\, e \in \text{DOMAIN } \mathit{cachePending}[c] :$
$\quad\quad \mathit{Cache}(c,\, e)$
$\lor \exists\, c \in \mathit{Client} :$
$\quad \mathit{Learn}(c)$
$\lor \exists\, c \in \mathit{Client} :$
$\quad \exists\, k \in \mathit{Key} :$
$\quad\quad \mathit{Evict}(c,\, k)$

$\mathit{Spec} \triangleq \mathit{Init} \land \Box[\mathit{Next}]_{\langle \mathit{vars} \rangle}$

* Modification History
* Last modified *Wed Feb* 12 17:20:34 *PST* 2020 by *jordanhalterman*
* Created *Mon Feb* 10 23:01:48 *PST* 2020 by *jordanhalterman*