On the correctness of monadic backward induction

NURIA BREDE
University of Potsdam, Potsdam, Germany
Potsdam Institute for Climate Impact Research, Potsdam, Germany
(e-mail: brede@uni-potsdam.de)

NICOLA BOTTA
Potsdam Institute for Climate Impact Research, Potsdam, Germany
Chalmers University of Technology, Göteborg, Sweden
(e-mail: boto@pik-potsdam.de)

Abstract

In control theory, to solve a finite-horizon sequential decision problem (SDP) commonly means to find a list of decision rules that result in an optimal expected total reward (or cost) when taking a given number of decision steps. SDPs are routinely solved using Bellman’s backward induction. Textbook authors (e.g. Bertsekas or Puterman) typically give more or less formal proofs to show that the backward induction algorithm is correct as solution method for deterministic and stochastic SDPs. Botta, Jansson and Ionescu propose a generic framework for finite horizon, monadic SDPs together with a monadic version of backward induction for solving such SDPs. In monadic SDPs, the monad captures a generic notion of uncertainty, while a generic measure function aggregates rewards. In the present paper, we define a notion of correctness for monadic SDPs and identify three conditions that allow us to prove a correctness result for monadic backward induction that is comparable to textbook correctness proofs for ordinary backward induction. The conditions that we impose are fairly general and can be cast in category-theoretical terms using the notion of Eilenberg–Moore algebra. They hold in familiar settings like those of deterministic or stochastic SDPs, but we also give examples in which they fail. Our results show that backward induction can safely be employed for a broader class of SDPs than usually treated in textbooks. However, they also rule out certain instances that were considered admissible in the context of Botta et al.’s generic framework. Our development is formalised in Idris as an extension of the Botta et al. framework and the sources are available as supplementary material.

1 Introduction

Backward induction is a method introduced by Bellman (1957) that is routinely used to solve finite-horizon sequential decision problems (SDPs). Such problems lie at the core of many applications in economics, logistics and computer science (Finus et al., 2003; Helm, 2003; Heitzig, 2012; Gintis, 2007; Botta et al., 2013; De Moor, 1995, 1999). Examples include inventory, scheduling and shortest path problems, but also the search for optimal strategies in games (Bertsekas, 1995; Diederich, 2001).
Botta, Jansson & Ionescu (2017a) propose a generic framework for monadic finite-horizon SDPs as generalisation of the deterministic, non-deterministic and stochastic SDPs treated in control theory textbooks (Bertsekas, 1995; Puterman, 2014). This framework allows to specify such problems and to solve them with a generic version of backward induction that we will refer to as monadic backward induction.

The Botta–Jansson–Ionescu-framework, subsequently referred to as BJI-framework, BJI-theory or simply framework, already includes a verification of monadic backward induction with respect to a certain underlying value function (see Section 3.2). However, in the literature on stochastic SDPs, this formulation of the function is itself part of the backward induction algorithm and needs to be verified against an optimisation criterion, the expected total reward (Puterman, 2014, Ch. 4.2). For stochastic SDPs semi-formal proofs can be found in textbooks – but monadic SDPs are substantially more general than the stochastic SDPs for which these results are established. This observation raises a number of questions:

- What exactly should “correctness” mean for a solution of monadic SDPs?
- Does monadic backward induction provide correct solutions in this sense for monadic SDPs in their full generality?
- And if not, is there a class of monadic SDPs for which monadic backward induction does provide provably correct solutions?

In the present paper, we address these questions and make the following contributions to answering them:

- We put forward a formal specification that monadic backward induction should meet in order to be considered “correct” as solution method for monadic SDPs. This specification uses an optimisation criterion that is a generic version of the expected total reward of standard control theory textbooks. In analogy, we call this criterion measured total reward.
- We consider the value function underlying monadic backward induction as “correct” if it computes the measured total reward.
- If the value function is correct, monadic backward induction can be proven to be correct in our sense by extending the result of Botta et al. (2017a). However, we show that this is not necessarily the case, i.e. the value function does not compute the measured total reward for arbitrary monadic SDPs.
- We therefore formulate conditions that identify a class of monadic SDPs for which the value function and thus monadic backward induction can be shown to be correct. The conditions are fairly simple and allow for a neat description in category-theoretical terms using the notion of Eilenberg-Moore-algebra.
- We give a formalised proof that monadic backward induction fulfils the correctness criterion if the conditions hold. This correctness result can be seen as a generic version of correctness results for standard backward induction like Bertsekas (1995, Prop. 1.3.1) and Puterman (2014, Th. 4.5.1.c).

1 Note that in control theory backward induction is often referred to as the dynamic programming algorithm where the term dynamic programming is used in the original sense of Bellman (1957).
Our results rule out the application of backward induction to certain monadic SDPs that were previously considered as admissible in the BJI-framework. Thus, they complement the verification result of Botta et al. and provide a necessary clarification. Still, the new conditions are simple enough to be checked for non-standard instantiations of the framework. This allows to broaden the applicability of backward induction to settings which are not commonly discussed in the literature and to obtain a formalised proof of correctness with considerably less effort. It is worth stressing that our conditions can be useful for anyone interested in applying monadic backward induction in non-standard situations – completely independent of the BJI-framework.

Finally, the value function underlying monadic backward induction is also interesting in itself. Given the conditions hold, it can be used to compute the measured total reward efficiently, using a method reminiscent of a thinning algorithm (Bird & Gibbons, 2020, Ch. 10).

For the reader unfamiliar with SDPs, we provide a brief informal overview and two simple examples in the next section. We recap the BJI-framework and its (partial) verification result for monadic backward induction in Section 3. In Section 4, we specify correctness for monadic backward induction and the BJI-value function. We also show that in the general monadic case the value function does not necessarily meet the specification. To resolve this problem, we identify conditions under which the value function does meet the specification. These conditions are stated and analysed in Section 5. In Section 6, we prove that, given the conditions hold, the BJI-value function and monadic backward induction are correct in the sense defined in Section 4. We discuss the conditions from a more abstract perspective in Section 7 and conclude in Section 8.

Throughout the paper, we use Idris as our host language (Brady, 2013, 2017). We assume some familiarity with Haskell-like syntax and notions like functor and monad as used in functional programming. We tacitly consider types as logical statements and programs as proofs, justified by the propositions-as-types correspondence (for an accessible introduction see Wadler, 2015).

**Source code.** Our development is formalised in Idris as an extension of a lightweight version of the BJI-framework. The proofs are machine-checked and the source code is available as supplementary material attached to this paper. The sources of this document have been written in literal Idris and are available at Brede & Botta (2021), together with some example code. All source files can be type checked with Idris 1.3.2.

## 2 Finite-horizon sequential decision problems

In deterministic, non-deterministic and stochastic finite-horizon SDPs, a decision maker seeks to control the evolution of a (dynamical) system at a finite number of decision steps by selecting certain controls in sequence, one after the other. The controls available to the decision maker at a given decision step typically depend on the state of the system at that step.

In deterministic problems, selecting a control in a state at decision step $t : \mathbb{N}$, determines a unique next state at decision step $t + 1$ through a given transition function. In
non-deterministic problems, the transition function yields a whole set of possible states at the next decision step. In stochastic problems, the transition function yields a probability distribution on states at the next decision step.

The notion of monadic problem generalises that of deterministic, non-deterministic and stochastic problem through a transition function that yields an $M$-structure of next states where $M$ is a monad. For example, the identity monad can be applied to model deterministic systems. Non-deterministic systems can be represented in terms of transition functions that return lists (or some other representations of sets) of next states. Stochastic systems can be represented in terms of probability distribution monads (Giry, 1981; Erwig & Kollmansberger, 2006; Audebaud & Paulin-Mohring, 2009; Jacobs, 2011). The uncertainty monad, the states, the controls and the next function define what is often called a decision process.

The idea of sequential decision problems is that each single decision yields a reward and these rewards add up to a total reward over all decision steps. Rewards are often represented by values of a numeric type and added up using the canonical addition. If the transition function and thus the evolution of the system is not deterministic, then the resulting possible total rewards need to be aggregated to yield a single outcome value. In stochastic SDPs, evolving the underlying stochastic system leads to a probability distribution on total rewards which is usually aggregated using the familiar expected value measure. The value thus obtained is called the expected total reward (Puterman, 2014, ch. 4.1.2) and its role is central: It is the quantity that is to be optimised in an SDP.

In monadic SDPs, the measure is generic, i.e. it is not fixed in advance but has to be given as part of the specification of a concrete problem. Therefore, we will generalise the notion of expected total reward to a corresponding notion for monadic SDPs that we call measured total reward in analogy (see Section 4).

Solving a stochastic SDP consists in finding a list of rules for selecting controls that maximises the expected total reward for $n$ decision steps when starting at decision step $t$. Similarly, we define that solving a monadic SDP consists in finding a list of rules for selecting controls that maximises the measured total reward. This means that when starting from any initial state at decision step $t$, following the computed list of rules for selecting controls will result in a value that is maximal as measure of the sum of rewards along all possible trajectories rooted in that initial state.

Equivalently, rewards can instead be considered as costs that need to be minimised. This dual perspective is taken e.g. in Bertsekas (1995). In the subsequent sections, we will follow the terminology of the BJI-framework and Puterman (2014) and speak of “rewards”, but our second example below will illustrate the “cost” perspective.

In mathematical theories of optimal control, the rules for selecting controls are called policies. A policy for a decision step is simply a function that maps each possible state to a control. As mentioned above, the controls available in a given state typically depend on that state, thus policies are dependently typed functions. A list of such policies is called a policy sequence.

The central idea underlying backward induction is to compute a globally optimal solution of a multi-step SDP incrementally by solving local optimisation problems at each decision step. This is captured by Bellman’s principle: Extending an optimal policy sequence with an optimal policy yields again an optimal policy sequence. However, as
Correctness of Monadic BI

(a) (b)

Fig. 1: Transition graphs for the example SDPs described in Section 2. The edge labels denote pairs control $\mid$ reward for the associated transitions. In the first example, state and control spaces are constant over time therefore we have omitted the temporal dimension.

we will see in Section 4.2, one has to carefully check whether for a given SDP backward induction is indeed applicable.

Two features are crucial for finite-horizon, monadic SDPs to be solvable with the BJI-framework that we study in this paper: (1) the number of decision steps has to be given explicitly as input to the backward induction and (2) at each decision step, the number of possible next states has to be finite. While (2) is a necessary condition for backward induction to be computable, (1) is a genuine limitation of the BJI-framework: in many SDPs, for example in a game of tic-tac-toe, the number of decision steps is bounded but not known a priori.

Before we discuss the BJI-framework in the next section, we illustrate the notion of sequential decision problem with two simple examples, one in which the purpose is to maximise rewards and one in which the purpose is to minimise costs. Rewards and costs in these examples are just natural numbers and are summed up with ordinary addition. The first example is a non-deterministic SDP. Although it is somewhat oversimplified, it has the advantage of being tractable for computations by hand while still being sufficient as basis for illustrations in Sections 3–5. The second example is a deterministic SDP that stands for the important class of scheduling SDPs. This problem highlights why dependent types are necessary to model state and control spaces accurately. As in these simple examples state and control spaces are finite, the transition functions can be described by directed graphs. These are given in Fig. 1.

Example 1 (A toy climate problem). Our first example is a variant of a stochastic climate science SDP studied in Botta et al. (2018), stripped down to a simple non-deterministic SDP. At every decision step, the world may be in one of two states, namely Good or Bad, and the controls determine whether a Low or a High amount of green house gases is
emitted into the atmosphere. If the world is in the Good state, choosing Low emissions will definitely keep the world in the Good state, but the result of choosing high emissions is non-deterministic: either the world may stay in the Good or tip to the Bad state. Similarly, in the Bad state, High emissions will definitely keep the world in Bad, while with Low emissions it might either stay in Bad or recover and return to the Good state. The transitions just described define a non-deterministic transition function. The rewards associated with each transition are determined by the respective control and reached state. Now we can formulate an SDP: “Which policy sequence will maximise the worst-case sum of rewards along all possible trajectories when taking n decisions starting at decision step t?” In this simple example, the question is not hard to answer: always choose Low emissions, independent of decision step and state. The optimal policy sequence for any n and t would thus consist of n constant Low functions. But in a more realistic example, the situation will be more involved: every option will have its benefits and drawbacks encoded in a more complicated reward function, uncertainties might come with different probabilities, there might be intermediate states, different combinations of control options, etc. For more along these lines, we refer the interested reader to Botta et al. (2018).

Example 2 (Scheduling). Scheduling problems serve as canonical examples in control theory textbooks. The one we present here is a slightly modified version of Bertsekas (1995, Example 1.1.2).

Think of some machine in a factory that can perform different operations, say A, B, C and D. Each of these operations is supposed to be performed once. The machine can only perform one operation at a time, thus an order has to be fixed in which to perform the operations. Setting the machine up for each operation incurs a specific cost that might vary according to which operation has been performed before. Moreover, operation B can only be performed after operation A has already been completed, and operation D only after operation C. It suffices to fix the order in which the first three operations are to be performed as this uniquely determines which will be the fourth task. The aim is now to choose an order that minimises the total cost of performing the four operations.

This situation can be modelled as follows as a problem with three decision steps: The states at each step are the sequences of operations already performed, with the empty sequence at step 0. The controls at a decision step and in a state are the operations which have not already been performed at previous steps and which are permitted in that state. For example, at decision step 0, only controls A and C are available because of the above constraint on performing B and D. The transition and cost functions of the problem are depicted by the graph in Figure 1b. As the problem is deterministic, picking a control will result in a unique next state and each sequence of policies will result in a unique trajectory. In this setting, solving the SDP reduces to finding a control sequence that minimises the sum of costs along the single resulting trajectory. In Figure 1b, this is the sequence CAB(D).

3 The BJI-framework

The BJI-framework is a dependently typed formalisation of optimal control theory for finite-horizon, discrete-time SDPs. It extends mathematical formulations for stochastic
SDPs (Bertsekas, 1995; Bertsekas & Shreve, 1996; Puterman, 2014) to the general problem of optimal decision making under monadic uncertainty.

For monadic SDPs, the framework provides a generic implementation of backward induction. It has been applied to study the impact of uncertainties on optimal emission policies (Botta et al., 2018) and is currently used to investigate solar radiation management problems under tipping point uncertainty (TiPES, 2019–2023).

In a nutshell, the framework consists of two sets of components: one for the specification of an SDP and one for its solution with monadic backward induction.

### 3.1 Problem specification components

In the following, we discuss the components necessary to specify a monadic SDP.

The first one is the monad \( M \):

\[
M : \text{Type} \rightarrow \text{Type}
\]

As discussed in the previous section, \( M \) accounts for the uncertainties that affect the decision problem. For our first example, we could for instance define \( M \) to be \( \text{List} \). For the second example it suffices to use \( M = \text{Id} \) as the problem is deterministic.

Further, the BJI-framework supports the specification of the states, the controls and the transition function of an SDP through

\[
X : (t : \mathbb{N}) \rightarrow \text{Type} \\
Y : (t : \mathbb{N}) \rightarrow X \rightarrow \text{Type} \\
\text{next} : (t : \mathbb{N}) \rightarrow (x : X \rightarrow Y \rightarrow M (X (S t)))
\]

The interpretation is that \( X t \) represents the states at decision step \( t \).

In the first example of Section 2, there are just two states (\( \text{Good} \) and \( \text{Bad} \)) such that \( X \) is a constant family:

\[
\text{data State} = \text{Good} \mid \text{Bad} \\
X_0 = \text{State}
\]

But in the second example the possible states depend on the decision step \( t \). Taking for example step \( t = 2 \), we could simply define

\[
\text{data State2} = \text{AB} \mid \text{AC} \mid \text{CA} \mid \text{CD} \\
X_2 = \text{State2}
\]

Alternatively, we could employ type dependency in a more systematic way to express that in Ex. 2 states are admissible sequences of actions

\[
\text{data Act} = \text{A} \mid \text{B} \mid \text{C} \mid \text{D}
\]

Recall that actions could require that another action was performed before, no action was to be carried out twice and the problem was limited to 3 steps. These conditions might be captured by a type-valued predicate

\[
\text{AdmissibleState} : \{t : \mathbb{N}\} \rightarrow \text{Vect} t \text{Act} \rightarrow \text{Type}
\]

and the type of states might then be expressed as dependent pair of a vector of actions and a proof that it is admissible.

---

2 Note that in Idris, \( S \) and \( Z \) are the familiar constructors of the data type \( \mathbb{N} \).
\[ X_t = (as : \text{Vect } t \text{ Act} \bowtie \text{AdmissibleState } as) \]

Similarly, \( Y_t x \) represents the controls available at decision step \( t \) and in state \( x \) and \( \text{next}_t x y \) represents the states that can be obtained by selecting control \( y \) in state \( x \) at decision step \( t \). In our first example, the available controls remain constant over time (High or Low) like the states, but for the second example, the type dependency is relevant: e.g. we might define (again at step \( t = 2 \))

\[
\text{data CtrlAC } = B \mid D
\]
\[
Y_2 AC = \text{CtrlAC}
\]

or more elegantly use dependent pairs to define the type of controls, using the observation that an action is an admissible control for some state represented by a vector of actions, if adding the action to the vector results again in an admissible state:

\[
\text{AdmissibleControl} : \{ t : \mathbb{N} \} \to \text{Vect } t \text{ Act} \to \text{Act} \to \text{Type}
\]
\[
\text{AdmissibleControl as } a = \text{AdmissibleState} (a :: as)
\]
\[
Y_t x = (a : \text{Act } \bowtie \text{AdmissibleControl} (\text{fst } x) a)
\]

Recall from Section 2 that the monad, the states, the controls and the next function together define a decision process. In order to fully specify a decision problem, one also has to define the rewards obtained at each decision step and the operation that is used to add up rewards. In the BJI-framework, this is done in terms of

\[
\text{Val} : \text{Type}
\]
\[
\text{reward} : (t : \mathbb{N}) \to (x : X_t) \to Y_t x \to X (S\ t) \to \text{Val}
\]
\[
(\odot) : \text{Val} \to \text{Val} \to \text{Val}
\]

Here, \( \text{Val} \) is the type of rewards and \( \text{reward } t x y x' \) is the reward obtained by selecting control \( y \) in state \( x \) if the next state is \( x' \), an element of the state space at step \( t + 1 \). Note that for deterministic problems it is unnecessary to parameterise the reward function over the next state as it is unique and can thus be obtained from the current state and control. But for non-deterministic problems, it is useful to be able to assign rewards depending on the (uncertain) outcome of a transition.

A few remarks are at place here.

- In many applications, \( \text{Val} \) is a numerical type and the controls of the SDP represent resources (fuel, water, etc.) that come at a cost. In these cases, the reward function encodes the costs and perhaps also the benefits associated with a decision step. Often, the latter also depends both on the current state \( x \) and on the next state \( x' \). The BJI-framework nicely copes with all these situations.
- The operation \( \odot \) determines how rewards are added up. It could be a simple arithmetic operation, but it could also be defined in terms of problem-specific parameters, e.g. discount factors to give more weight to current rewards as compared to future rewards.
- Mapping \( \text{reward } t x y \) onto \( \text{next}_t x y \) (remember that \( M \) is a monad and thus a functor) yields a value of type \( M \text{ Val} \). These are the possible rewards obtained by selecting control \( y \) in state \( x \) at decision step \( t \). In mathematical theories of optimal control, the implicit assumption often is that \( \text{Val} \) is equal to \( \mathbb{R} \) and that the \( M \)-structure is a
Formalisation of Ex. 1:

We use the monoid and preorder structure on $\mathbb{N}$, i.e. $Val = \mathbb{N}$, $(\oplus) = (+)$, $zero = 0$, $(\leq) = (\subseteq)$.

$M = List$

Measure:

$minList : List \mathbb{N} \rightarrow \mathbb{N}$

$minList [] = 0$

$minList (x :: []) = x$

$minList (x :: xs) = x \cdot \text{'minimum'} \cdot xs$

$meas = minList$

States and Controls:

$\text{data States = Good | Bad}$

$\text{data Controls = High | Low}$

$X \downarrow = \text{States}$

$Y \downarrow \cdot x = \text{Controls}$

Transition function:

$next \downarrow \cdot \text{Good Low} = \text{Good}$

$next \downarrow \cdot \text{Bad High} = \text{Bad}$

$next \downarrow \cdot x \downarrow \cdot y = \text{Good, Bad}$

Rewards:

$\text{reward } \downarrow \cdot x \downarrow \cdot \text{Low Good} = 3$

$\text{reward } \downarrow \cdot x \downarrow \cdot \text{High Good} = 2$

$\text{reward } \downarrow \cdot x \downarrow \cdot \text{Low Bad} = 1$

$\text{reward } \downarrow \cdot x \downarrow \cdot \text{High Bad} = 0$

Fig. 2: A formalisation of Ex. 1 from Section 2.

probability distribution on real numbers which can be evaluated with the expected value measure. However, in many practical applications, measuring uncertainty of rewards in terms of the expected value is inadequate (Mercure et al., 2020). The BJI-framework therefore takes a generic approach and allows the specification of SDPs in terms of problem-specific measures.

As just discussed, in SDPs with uncertainty a measure is required to aggregate multiple possible rewards. The BJI-framework supports the specification of the measure by:

$meas : M Val \rightarrow Val$

In our first example we could use the minimum of a list as worst-case measure, while in the second example the measure would just be the identity (as the problem is deterministic).

Before we get to the solution components of the BJI-framework, one more ingredient needs to be specified. In the next section, we will formalise a notion of optimality for which it is necessary to be able to compare elements of $Val$. The framework allows users to compare $Val$-values in terms of a problem specific comparison operator:

$(\sqsubseteq) : Val \rightarrow Val \rightarrow Type$

The operator $(\sqsubseteq)$ is required to define a total preorder on $Val$. In our two examples, we simply have:

$Val = \mathbb{N}$

$(\oplus) = (+)$

$(\sqsubseteq) = (\leq)$

Three more ingredients are necessary to fully specify a monadic SDP, but we defer discussing them to when they come up in the next subsection. For illustration, a formalisation of Ex. 1 can be found in Fig. 2. A formalisation of Ex. 2 is included in the supplementary material.
3.2 Problem solution components

The second set of components of the BJI-framework is an extension of the mathematical theory of optimal control for stochastic sequential decision problems to monadic problems. Here, we provide a summary of the theory. Motivation and full details can be found in Botta et al. (2017a,b, 2018).

The theory formalises the notions of policy (decision rule) from Section 2 as

\[ Policy : (t : \mathbb{N}) \to Type \]
\[ Policy t = (x : X t) \to Y t x \]

Policy sequences are then essentially vectors of policies\(^3\).

\[ data PolicySeq : (t, n : \mathbb{N}) \to Type \]
\[ Nil : \{ t : \mathbb{N} \} \to PolicySeq t Z \]
\[ (::) : \{ t, n : \mathbb{N} \} \to Policy t \to PolicySeq (S t) n \to PolicySeq t (S n) \]

Notice the role of the step (time) index \( t \) and of the length index \( n \) in the constructors of policy sequences: For a policy sequence to make sense, policies for taking decisions at step \( t \) can only be prepended to policy sequences for taking first decisions at step \( t + 1 \) and the operation yields policy sequences for taking first decisions at step \( t \). Thus, the time index allows to ensure a consistency property of policy sequences by construction. As for plain vectors and lists, prepending a policy to a policy sequence of length \( n \) yields a policy sequence of length \( n + 1 \). Both the time and the length index will be useful below: they allow to express that the backward induction algorithm computes policy sequences starting at a specific time and having a specific length depending on its inputs.

The perhaps most important ingredient of backward induction is a value function that incrementally measures and adds up rewards. For a given decision problem, the value function takes two arguments: a policy sequence \( ps \) for making \( n \) decision steps starting from decision step \( t \) and an initial state \( x : X t \). It computes the value of taking \( n \) decision steps according to the policies \( ps \) when starting in \( x \). In the BJI-framework, the value function is defined as

\[ val : \{ t, n : \mathbb{N} \} \to PolicySeq t n \to X t \to Val \]
\[ val \{ t \} Nil x = zero \]
\[ val \{ t \} (p :: ps) x = let y = p x in \]
\[ let mx' = next t x y in \]
\[ meas (map (reward t x y \oplus val ps) mx') \]

Notice that, independently of the initial state \( x \), the value of the empty policy sequence is \( zero \). This is a problem-specific reference value

\[ zero : Val \]

that has to be provided as part of a problem specification.\(^4\) It is one of the specification components that we have not discussed in Section 3.1. The value of a policy sequence consisting of a first policy \( p \) and of a tail policy sequence \( ps \) is defined inductively as

\(^3\) The curly brackets in the types of \( Nil \) and \( :: \) indicate that \( t \) and \( n \) are implicit arguments.
\(^4\) The name might suggest that \( zero \) is supposed to be a neutral element relative to \( \oplus \). However, this is not required by the framework.
the measure of an $M$-structure of $Val$-values. These values are obtained by first computing the control $y$ dictated by the policy $p$ in state $x$ and the $M$-structure of possible next states $mx'$ dictated by the transition function $next$. Then, for all $x'$ in $mx'$ the current reward $t 	imes y 	imes x'$ is added to the aggregated outcome for the tail policy sequence $val ps x'$. Finally, the result of this functorial mapping is aggregated with the problem-specific measure $meas$ to obtain a result of type $Val$ as outcome for the policy sequence $(p :: ps)$. The function which is mapped onto $mx'$ is just a lifted version of $\oplus$:

$$(\oplus): \{A : Type\} \rightarrow (f, g : A \rightarrow Val) \rightarrow A \rightarrow Val$$

$$f \oplus g = \lambda a \rightarrow f a \oplus g a$$

We will come back to the value function of the BJI-theory in Section 4 where we will contrast it with a function $val'$ that, for a policy sequence $ps$ and an initial state $x$, computes the measure of the sum of the rewards along all possible trajectories starting at $x$ under $ps$ (the measured total reward that we anticipated in Section 2). For the time being, though, we accept the notion of value of a policy sequence as put forward in the BJI-theory and we show how the definition of $val$ can be employed to compute policy sequences that are provably optimal in the sense of

$$OptPolicySeq : \{t, n : \mathbb{N}\} \rightarrow PolicySeq t n \rightarrow Type$$

$$OptPolicySeq \{t\} \{n\} ps = (ps' : PolicySeq t n) \rightarrow (x : X t) \rightarrow val ps' x \subseteq val ps x$$

Notice the universal quantification in this definition: A policy sequence $ps$ is defined to be optimal iff $val ps' x \subseteq val ps x$ for any policy sequence $ps'$ and for any state $x$.

The generic implementation of backward induction in the BJI-framework is an application of Bellman’s principle of optimality mentioned in Section 2. In control theory textbooks, this principle is often referred to as Bellman’s equation. It can be suitably formulated in terms of the notion of optimal extension. We say that a policy $p : Policy t$ is an optimal extension of a policy sequence $ps : Policy (S t) n$ if it is the case that the value of $p :: ps$ is at least as good as the value of $p' :: ps$ for any policy $p'$ and for any state $x : X t$:

$$OptExt : \{t, n : \mathbb{N}\} \rightarrow PolicySeq (S t) n \rightarrow Policy t \rightarrow Type$$

$$OptExt \{t\} ps p = (p' : Policy t) \rightarrow (x : X t) \rightarrow val (p' :: ps)x \subseteq val (p :: ps)x$$

With the notion of optimal extension in place, Bellman’s principle can be formulated as

$$Bellman : \{t, n : \mathbb{N}\} \rightarrow$$

$$(ps : PolicySeq (S t) n) \rightarrow OptPolicySeq ps \rightarrow$$

$$(p : Policy t) \rightarrow OptExt ps p \rightarrow$$

$$OptPolicySeq (p :: ps)$$

In words: extending an optimal policy sequence with an optimal extension (of that policy sequence) yields an optimal policy sequence or shorter prefixing with optimal extensions preserves optimality. Proving Bellman’s optimality principle is almost straightforward and relies on $\sqsubseteq$ being reflexive and transitive and two monotonicity properties:

$$plusMonSpec : \{v1, v2, v3, v4 : Val\} \rightarrow v1 \sqsubseteq v2 \rightarrow v3 \sqsubseteq v4 \rightarrow (v1 \oplus v3) \sqsubseteq (v2 \oplus v4)$$

$$measMonSpec : \{A : Type\} \rightarrow (f, g : A \rightarrow Val) \rightarrow ((a : A) \rightarrow f a \sqsubseteq g a) \rightarrow$$

$$(ma : MA) \rightarrow meas (map f ma) \sqsubseteq meas (map g ma)$$

The second condition is a special case of the measure monotonicity requirement originally formulated by Ionescu (2009) in the context of a theory of vulnerability and monadic
It is a natural property and the expected value measure, the worst-
(best) case measure and any sound statistical measure fulfil it. Like the reference value
zero discussed above, plusMonSpec and measMonSpec are specification components of the
BJI-framework that we have not discussed in Section 3.1. We provide a proof of Bellman
in Appendix 5. As one would expect, the proof makes essential use of the recursive defi-
nition of the function val discussed above. As a consequence, this precise definition of val
plays a crucial role for the verification of backward induction in Botta et al. (2017a).

Apart from the increased level of generality, the definition of val and Bellman are in fact
just an Idris formalisation of Bellman’s equation as formulated in control theory textbooks.
With Bellman and provided that we can compute optimal extensions of arbitrary policy
sequences

\[
\text{optExt} : \{t, n : \mathbb{N}\} \rightarrow \text{PolicySeq} (S t) n \rightarrow \text{Policy}
\]

\[
\text{optExtSpec} : \{t, n : \mathbb{N}\} \rightarrow (ps : \text{PolicySeq} (S t) n) \rightarrow \text{OptExt} ps (\text{optExt} ps)
\]

it is easy to derive an implementation of monadic backward induction that computes
provably optimal policy sequences with respect to val: first, notice that the empty policy
sequence is optimal:

\[
\text{nilOptPolicySeq} : \text{OptPolicySeq} \text{Nil}
\]

\[
\text{nilOptPolicySeq} \text{ Nil} x = \text{reflexive} \text{ lteTP} \text{ zero}
\]

This is the base case for constructing optimal policy sequences by backward induction,
starting from the empty policy sequence:

\[
\text{bi} : (t, n : \mathbb{N}) \rightarrow \text{PolicySeq} t n
\]

\[
\text{bi} t \ Z = \text{Nil}
\]

\[
\text{bi} t (S n) = \text{let} \ ps = \text{bi} (S t) n \text{ in} \ \text{optExt} ps :: ps
\]

That bi computes optimal policy sequences with respect to val is then proved by induction
on n, the input that determines the length of the resulting policy sequence:

\[
\text{biOptVal} : (t, n : \mathbb{N}) \rightarrow \text{OptPolicySeq} (\text{bi} t n)
\]

\[
\text{biOptVal} t \ Z = \text{nilOptPolicySeq}
\]

\[
\text{biOptVal} t (S n) = \text{Bellman} \ ps \ ops \ p \ oep \ \text{where}
\]

\[
ps : \text{PolicySeq} (S t) n ; \quad ps = \text{bi} (S t) n
\]

\[
ops : \text{OptPolicySeq} ps ; \quad ops = \text{biOptVal} (S t) n
\]

\[
p : \text{Policy} t ; \quad p = \text{optExt} ps
\]

\[
oep : \text{OptExt} ps p ; \quad oep = \text{optExtSpec} ps
\]

This is the verification result for bi of Botta et al. (2017a).5

3.3 BJI-framework wrap-up

The specification and solution components discussed in the last two sections are all we
need to formulate precisely the problem of correctness for monadic backward induction
in the BJI-framework. This is done in the next section. Before turning to it, two further
remarks are necessary:

5 Note that biOptVal is called biLemma in Botta et al. (2017a). We chose the new name to emphasise that bi
computes optimal policy sequences with respect to val.
The theory proposed in Botta et al. (2017a) is slightly more general than the one summarised above. Here, policies are just functions from states to controls:

\[
\text{Policy} : (t : \mathbb{N}) \rightarrow \text{Type} \\
\text{Policy} t = (x : X t) \rightarrow Y t x
\]

By contrast, in Botta et al. (2017a), policies are indexed over a number of decision steps \(n\)

\[
\text{Policy} : (t, n : \mathbb{N}) \rightarrow \text{Type} \\
\text{Policy} t \text{Z} = \text{Unit} \\
\text{Policy} t (S m) = (x : X t) \rightarrow \text{Reachable} x \rightarrow \text{Viable} (S m) x \rightarrow \text{GoodCtrl} t x m
\]

and their domain for \(n > 0\) is restricted to states that are reachable and viable for \(n\) steps. This allows to cope with states whose control set is empty and with transition functions that return empty \(M\)-structures of next states. (For a discussion of reachability and viability see Botta et al. 2017a, Sections 3.7 and 3.8.)

This generality, however, comes at a cost: Compare, e.g. the proof of Bellman’s principle from the last subsection with the corresponding proof in Botta et al. (2017a, Appendix B). The impact of the reachability and viability constraints on other parts of the theory is even more severe.

Here, we have decided to trade some generality for better readability and opted for a simplified version of the original theory. Still, for the generic backward induction algorithm we need to make sure that it is possible to define policy sequences of the length required for a specific SDP. This can, e.g. be done by postulating controls to be non-empty:

\[
\text{notEmptyY} : (t : \mathbb{N}) \rightarrow (x : X t) \rightarrow Y t x
\]

We also impose a non-emptiness requirement on the transition function \(\text{next}\) that will be discussed in Section 7.

\[
\text{nextNotEmpty} : \{ t : \mathbb{N} \} \rightarrow (x : X t) \rightarrow (y : Y t x) \rightarrow \text{NotEmpty} (\text{next} t x y)
\]

In Section 3.2, we have not discussed under which conditions one can implement optimal extensions of arbitrary policy sequences. This is an interesting topic that is however orthogonal to the purpose of the current paper. For the same reason, we have not addressed the question of how to make \(\text{bi}\) more efficient by tabulation. We briefly discuss the specification and implementation of optimal extensions in the BJI-framework in Appendix 7. We refer the reader interested in tabulation of \(\text{bi}\) to SequentialDecisionProblems.TabBackwardsInduction of Botta (2016–2021).

4 Correctness for monadic backward induction

In this section, we formally specify the notions of correctness for monadic backward induction \(\text{bi}\) and the value function \(\text{val}\) of the BJI-framework that we will study in the remainder of this paper. We develop these notions as generic variants of the corresponding notions for stochastic SDPs.
4.1 Extension of the BJI-framework

In the previous section, we have seen that a monadic SDP can be specified in terms of nine components: \( M, X, Y, \text{next}, \text{Val}, \text{zero}, \oplus, \sqsubseteq \) and \( \text{reward} \).

Given a policy sequence (optimal or not) and an initial state for an SDP, we can compute the \( M \)-structure of possible trajectories starting at that state:

\[
\text{data StateCtrlSeq} : (t, n : \mathbb{N}) \to \text{Type}
\text{where}
\begin{align*}
\text{Last} & : (t : \mathbb{N}) \to X \to \text{StateCtrlSeq} t (SZ) \\
(\#) & : (t, n : \mathbb{N}) \to X \to X \ast Y \to \text{StateCtrlSeq} (S t) (S n) \to \text{StateCtrlSeq} t (S (S n))
\end{align*}
\]

\[
\text{trj} : (t, n : \mathbb{N}) \to \text{PolicySeq} t n \to X \to M \text{StateCtrlSeq} t (S n)
\text{trj} \{ t \} \text{Nil} x = \text{pure} (\text{Last} x)
\text{trj} \{ t \} (p :: ps) x = \text{let}
\quad y = px
\quad \text{let}
\quad mx' = \text{next} t x y
\quad \text{let}
\quad \text{map} ((x \ast y)\#\#)(mx' >\Rightarrow \text{trj} \text{ps})
\]

where we use \( \text{StateCtrlSeq} \) as type of trajectories. Essentially, it is a non-empty list of (dependent) state/control pairs, with the exception of the base case which is a singleton just containing the last state reached.

Furthermore, we can compute the total reward for a single trajectory, i.e. its sum of rewards:

\[
\text{sumR} : (t, n : \mathbb{N}) \to \text{StateCtrlSeq} t n \to \text{Val}
\text{sumR} \{ t \} \text{Last} x = \text{zero}
\text{sumR} \{ t \} ((x \ast y)\#\#) \text{xs} = \text{reward} t x y (\text{head} \text{xs}) \oplus \text{sumR} \text{xs}
\]

where \( \text{head} \) is the helper function

\[
\text{head} : (t, n : \mathbb{N}) \to \text{StateCtrlSeq} t (S n) \to X
\text{head} \text{Last} x = x
\text{head} ((x \ast y)\#\#) \text{xs} = x
\]

By mapping \( \text{sumR} \) onto an \( M \)-structure of trajectories, we obtain an \( M \)-structure containing the individual sums of rewards of the trajectories. Now, using the measure function, we can compute the generic analogue of the expected total reward for a policy sequence \( ps \) and an initial state \( x \):

\[
\text{val'} : (t, n : \mathbb{N}) \to (ps : \text{PolicySeq} t n) \to X \to \text{Val}
\text{val'} ps = \text{meas} \circ \text{map} \text{sumR} \circ \text{trj} \text{ps}
\]

As anticipated in Section 2, we call the value computed by \( \text{val'} \) the measured total reward. Recall that solving a stochastic SDP commonly means finding a policy sequence that maximises the expected total reward. By analogy, we define that solving a monadic SDP means to find a policy sequence that maximises the measured total reward. That is, given \( t \) and \( n \), the solution of a monadic SDP is a sequence of \( n \) policies that maximises the measure of the sum of rewards along all possible trajectories of length \( n \) that are rooted in an initial state at step \( t \).

Again by analogy to the stochastic case, we define monadic backward induction to be correct if, for a given SDP, the policy sequence computed by \( bi \) is the solution to the SDP. That is, we consider \( bi \) to be correct if it meets the specification

\[
\text{biOptMeasTotalReward} : (t, n : \mathbb{N}) \to \text{GenOptPolicySeq} \text{val'} (bi \ t \ n)
\]
where \( \text{GenOptPolicySeq} \) is a generalised version of the optimality predicate \( \text{OptPolicySeq} \) from Section 3.2. It now takes as an additional parameter the function with respect to which the policy sequence is to be optimal:

\[
\text{GenOptPolicySeq} : \{ t, n : \mathbb{N} \} \rightarrow (\text{PolicySeq} t n \rightarrow X t \rightarrow \text{Val}) \rightarrow \text{PolicySeq} t n \rightarrow \text{Type}
\]

As recapitulated in Section 3.2, Botta et al. have already shown that if \( M \) is a monad, \( \sqsubseteq \) a total preorder and \( \oplus \) and \( \text{meas} \) fulfil two monotonicity conditions, then \( \text{bi} t n \) yields an optimal policy sequence with respect to the value function \( \text{val} \) in the sense that

\[
\text{val} \, ps' \, x \sqsubseteq \text{val} \, (\text{bi} \, t \, n) \, x
\]

for any policy sequence \( ps' \) and initial state \( x \), for arbitrary \( t, n : \mathbb{N} \). Or, expressed using the generalised optimality predicate, that the type

\[
\text{GenOptPolicySeq} \{ t \} \{ n \} \, \text{val} \, (\text{bi} \, t \, n)
\]

is inhabited. As seen in Section 3.2, the function \( \text{val} \) measures and adds rewards incrementally. But does it always compute the measured total reward like \( \text{val}' \)? Modulo differences in the presentation Puterman (2014, Theorem 4.2.1) suggests that for standard stochastic SDPs, \( \text{val} \) and \( \text{val}' \) are extensionally equal, which in turn allows the use of backward induction for solving these SDPs. Generalising, we therefore consider \( \text{val} \) as correct if it fulfils the specification

\[
\text{valMeasTotalReward} : \{ t, n : \mathbb{N} \} \rightarrow (ps : \text{PolicySeq} \, t \, n) \rightarrow (x : X \, t) \rightarrow \text{val} \, ps \, x = \text{val}' \, ps \, x
\]

If this equality held for the general monadic SDPs of the BJI-theory, we could prove the correctness of \( \text{bi} \) as immediate corollary of \( \text{valMeasTotalReward} \) and Botta et al.’s result \( \text{biOptVal} \). The statement \( \text{biOptMeasTotalReward} \) can be seen as a generic version of textbook correctness statements for backward induction as solution method for stochastic SDPs like (Bertsekas 1995, prop.1.3.1) or Puterman (2014, Theorem 4.5.1.c). By proving \( \text{valMeasTotalReward} \), we could therefore extend the verification of Botta et al. (2017a) and obtain a stronger correctness result for monadic backward induction.

Our main objective in the remainder of the paper is therefore to prove that \( \text{valMeasTotalReward} \) holds. But there is a problem.

### 4.2 The problem with the BJI-value function

A closer look at \( \text{val} \) and \( \text{val}' \) reveals two quite different computational patterns: applied to a policy sequence \( ps \) of length \( n + 1 \) and a state \( x \), the function \( \text{val} \) directly evaluates \( \text{meas} \) on the \( M \)-structure of rewards corresponding to the possible next states after one step. This entails further evaluations of \( \text{meas} \) for each possible next state. By contrast, \( \text{val}' \, ps \, x \) entails only one evaluation of \( \text{meas} \), independently of the length of \( ps \). The computation, however, builds up an intermediate \( M \)-structure of state-control sequences. The elements of this \( M \)-structure, the state-control sequences, are then consumed by \( \text{sumR} \) and finally the \( M \)-structure of rewards is reduced by \( \text{meas} \).

For illustration, let us revisit Ex. 1 from Section 2 as formalised in Figure 2. To do an example calculation with \( \text{val} \) and \( \text{val}' \) we first need a concrete policy sequence as input. The simplest two policies are the two constant policies:
\[ \text{constH} : \langle t : \mathbb{N} \rangle \rightarrow \text{Policy} \]
\[ \text{constH}_t = \text{const High} \]
\[ \text{constL} : \langle t : \mathbb{N} \rangle \rightarrow \text{Policy} \]
\[ \text{constL}_t = \text{const Low} \]

From these, we can define a policy sequence

\[ ps : \text{PolicySeq} 0 3 \]
\[ ps = \text{constH} 0 :: (\text{constL} 1 :: (\text{constH} 2 :: \text{Nil})) \]

It is instructive to compute \( \text{val} \ ps \ \text{Good} \) and \( \text{val}' \ ps \ \text{Good} \) by hand. Recall that in this example, we have \( M = \text{List} \) with \( (\Rightarrow) = \text{concatMap} \) and \( \text{Val} = \mathbb{N} \) with \( \oplus = + \). The measure \( \text{meas} \) thus needs to have the type \( \text{List} \mathbb{N} \rightarrow \mathbb{N} \). Without instantiating \( \text{meas} \) for the moment, the computations roughly exhibit the structure

\[ \text{val} \ ps \ \text{Good} = \text{meas} [2 + \text{meas} [3 + \text{meas} [2, 0]], 0 + \text{meas} [3 + \text{meas} [2, 0], 1 + \text{meas} [0]]] \]
\[ \text{val}' \ ps \ \text{Good} = \text{meas} [7, 5, 5, 3, 1] \]

and it is not “obviously clear” that \( \text{val} \) and \( \text{val}' \) are extensionally equal without further knowledge about \( \text{meas} \).

In the deterministic case, i.e. for \( M = \text{Id} \) and \( \text{meas} = \text{id} \), \( \text{val} \ ps \ x \) and \( \text{val}' \ ps \ x \) are indeed equal for all \( ps \) and \( x \), without imposing any further conditions (as we will see in Section 6). For the stochastic case, (Puterman, 2014, Theorem 4.2.1) suggests that the equality should hold. But for the monadic case, no such result has been established. And as it turns out, in general the functions \( \text{val} \) and \( \text{val}' \) are not unconditionally equal – consider the following counter-example: We continue in the setting of Ex. 1 from above, but now instantiate the measure to the plain arithmetic sum

\[ \text{meas} = \text{foldr} (+) 0 \]

This measure fulfils the monotonicity condition (\( \text{measMonSpec} \), Section 3.2) imposed by the BJI-framework. But if we instantiate the above computations with it, then we get \( \text{val} \ ps \ \text{Good} = 13 \) and \( \text{val}' \ ps \ \text{Good} = 21! \) We thus see that the equality between \( \text{val} \) and \( \text{val}' \) cannot hold unconditionally in the generic setting of the BJI-framework. In the next section, we therefore present conditions under which the equality \textit{does} hold.

### 5 Correctness conditions

We now formulate three conditions on combinations of the monad, the measure function and the binary operation \( \oplus \) that imply the extensional equality of \( \text{val} \) and \( \text{val}' \):

**Condition 1.** The measure needs to be left-inverse to \( \text{pure} \): \(^6\)

\[ \text{measPureSpec} : \text{meas} \circ \text{pure} \rightleftharpoons \text{id} \]

\[ \begin{array}{c}
\text{Val} \\
\text{pure}
\end{array} \xrightarrow{\text{id}} \begin{array}{c}
\text{Val} \\
\text{meas}
\end{array} \]

\[ MVal \xrightarrow{\text{meas}} Val \]

\(^6\) The symbol \( \rightleftharpoons \) denotes \textit{extensional} equality, see Appendix 1.2
**Condition 2.** Applying the measure after \( \text{join} \) needs to be extensionally equal to applying it after \( \text{map meas} \):

\[
\text{measJoinSpec : } \text{meas} \circ \text{join} \cong \text{meas} \circ \text{map meas}
\]

\[
\begin{array}{c}
\text{M(Val)} \xrightarrow{\text{map meas}} \text{MVal} \\
\text{join} \downarrow \quad \downarrow \text{meas} \\
\text{MVal} \xrightarrow{\text{meas}} \text{Val}
\end{array}
\]

**Condition 3.** For arbitrary \( v : \text{Val} \) and non-empty \( mv : \text{MVal} \) applying the measure after mapping \((v \oplus)\) onto \( mv \) needs to be equal to applying \((v \oplus)\) after the measure:

\[
\text{measPlusSpec : } (v : \text{Val}) \rightarrow (mv : \text{MVal}) \rightarrow (\text{NotEmpty} mv) \rightarrow \\
(\text{meas} \circ \text{map } (v \oplus)) \text{mv } = ((v \oplus) \circ \text{meas}) \text{mv}
\]

\[
\begin{array}{c}
\text{MVal} \xrightarrow{\text{map}(v \oplus)} \text{MVal} \\
\text{meas} \downarrow \quad \downarrow \text{meas} \\
\text{Val} \xrightarrow{(v \oplus)} \text{Val}
\end{array}
\]

Essentially, these conditions assure that the measure is well-behaved relative to the monad structure and the \( \oplus \)-operation. They arise by, again, generalising from the standard example of stochastic SDPs with a probability monad, the expected value as measure and ordinary addition as \( \oplus \). The first two conditions are lifting properties that allow to do computations either in the monad or the underlying structure with the same result. The third condition is a distributivity law. For the computation of the measured total reward, it means that instead of adding the current reward to the outcome of each trajectory and then measuring, one may as well first measure the outcomes and then add the current reward.

To illustrate the conditions, let us consider a simple representation of discrete probability distributions like in Erwig & Kollmansberger (2006).

\[
\text{Dist : Type} \rightarrow \text{Type} \\
\text{Dist Omega} = \text{List (Omega, Double)}
\]

with

\[
\text{distMap : } \{A, B : \text{Type}\} \rightarrow (f : A \rightarrow B) \rightarrow \text{Dist A} \rightarrow \text{Dist B} \\
\text{distMap } f \text{ aps } = [(f \text{ (fst ap), snd ap) } | \text{ ap } \leftarrow \text{aps}]
\]

\[
\text{distPure : } \{A : \text{Type}\} \rightarrow A \rightarrow \text{Dist A} \\
\text{distPure } a = [(a, 1.0)]
\]

\[
\text{distJoin : } \{A : \text{Type}\} \rightarrow (\text{Dist (Dist A)}) \rightarrow \text{Dist A} \\
\text{distJoin apsps } = \text{concat } \left[(\text{fst ap, snd ap } \ast \text{snd aps)} \mid \text{ ap } \leftarrow \text{fst aps}, \text{ aps } \leftarrow \text{apsps}\right]
\]

\[
\text{Val = Double} \text{ and as measure the expected value} \\
\text{expected : Dist Double } \rightarrow \text{Double} \\
\text{expected dps } = \text{sum } \left[(\text{fst dp, snd dp } \ast \text{dp)} \mid \text{ dp } \leftarrow \text{dps}\right]
\]

With \( \text{meas } = \text{expected} \) and \( \oplus = + \), we can now consider the three conditions from above.
**Condition 1.** The first condition $\text{measPureSpec}$ holds since $1.0$ is neutral for $\ast$.

$$\text{expected} \circ \text{distPure} a = a \ast 1.0 = a$$

The second and the third condition require some arithmetic reasoning, so let us just consider them for two examples. Let $a, b, c, d$ be variables of type $\text{Double}$ and say we have distributions

$$dps1 : \text{Dist Double}$$
$$dps1 = [(a, 0.5), (b, 0.3), (c, 0.2)]$$

$$dps2 : \text{Dist Double}$$
$$dps2 = [(a, 0.4), (d, 0.6)]$$

$$dpdps : \text{Dist (Dist Double)}$$
$$dpdps = [(dps1, 0.1), (dps2, 0.9)]$$

**Condition 2.** Then the second condition $\text{measJoinSpec}$ instantiates to

$$(\text{expected} \circ \text{distJoin}) dpdps = (\text{expected} \circ \text{distMap expected}) dpdps$$

This equality holds because of the standard properties of addition and multiplication:

$$(\text{expected} \circ \text{distJoin}) dpdps =$$
$$\text{expected} [(a, 0.5 \ast 0.1), (b, 0.3 \ast 0.1), (c, 0.2 \ast 0.1), (a, 0.4 \ast 0.9), (d, 0.6 \ast 0.9)] =$$
$$(a \ast 0.5 \ast 0.1) + (b \ast 0.3 \ast 0.1) + (c \ast 0.2 \ast 0.1) + (a \ast 0.4 \ast 0.9) + (d \ast 0.6 \ast 0.9) =$$
$$((a \ast 0.5 + b \ast 0.3 + c \ast 0.2) \ast 0.1 + (a \ast 0.4 + d \ast 0.6) \ast 0.9) =$$
$$\text{expected} [(a \ast 0.5 + b \ast 0.3 + c \ast 0.2, 0.1), (a \ast 0.4 + d \ast 0.6, 0.9)] =$$
$$(\text{expected} \circ \text{distMap expected}) dpdps$$

**Condition 3.** For the third condition $\text{measPlusSpec}$, consider for some $v : \text{Double}$ the equation

$$(\text{expected} \circ \text{distMap} (v+)) dps1 = ((v+) \circ \text{expected}) dps1$$

Again using the usual arithmetic laws for $+$ and $\ast$, we can calculate

$$\text{expected} (\text{distMap} (v+)) [(a, 0.5), (b, 0.3), (c, 0.2)] =$$
$$(v + a) \ast 0.5 + (v + b) \ast 0.3 + (v + c) \ast 0.2 =$$
$$(v \ast 0.5 + a \ast 0.5) + (v \ast 0.3 + b \ast 0.3) + (v \ast 0.2 + c \ast 0.2) =$$
$$(v \ast 0.5 + v \ast 0.3 + v \ast 0.2) + (a \ast 0.5 + b \ast 0.3 + c \ast 0.2) =$$
$$v + \text{expected} [(a, 0.5), (b, 0.3), (c, 0.2)]$$

As we can see, an essential ingredient for the equality to hold is that the mapped occurrences of $(v+)$ are weighted by the probabilities which add up to 1.

Note that in this example, we have glossed over problems that might arise from the use of $\text{Dist}$ to represent probability distributions. We will briefly address probability monads and the expected value from a more abstract perspective in Subsection 5.2.

---

7 For the sake of simplicity, we do not address (important) conceptional questions concerning the representation of probability distributions or the problems caused by the use of floating point arithmetic in this example. Note,
5.1 Examples and counter-examples

Besides the motivating example above, let us now consider some more functions that have the correct type to serve as a measure, and that do or do not fulfil the three conditions.

Simple examples of admissible measures are the minimum \((\text{minList} \text{ as defined in Figure 2})\) or maximum \((\text{maxList} = \text{foldr 'maximum' 0})\) of a list for \(M = \text{List}\) with \(\mathbb{N}\) as type of values and ordinary addition as \(\oplus\). It is straightforward to prove that the conditions hold for these two measures and the proofs for \(\text{maxList}\) are included in the supplementary material.

The function \(\text{length}\) is a very simple counter-example: It has the right type for a list measure but fails all three of the conditions. As to other counter-examples, let us revisit the conditions one by one. Throughout, we use \(M = \text{List}\) with \(\text{map} = \text{listMap}, \text{join} = \text{concat}\) and \(\oplus = +\) (the canonical addition for the respective type of \(Val\)).

**Condition 1.** We remain in the setting of Ex. 1 with \(Val = \mathbb{N}\) and just vary the measure. Using a somewhat contrived variation of \(\text{maxList}\)

\[
\text{maxListVar} : \text{List} \mathbb{N} \rightarrow \mathbb{N} \quad \text{maxListVar} = \text{foldr} (\lambda x, v \Rightarrow (x + 1 \ 'maximum' v)) 0
\]

with \(meas = \text{maxListVar}\) it suffices to consider that for an arbitrary \(n : \mathbb{N}\)

\[
(\text{maxListVar} \circ \text{pure}) n = \text{maxListVar} [n] = (n + 1) \ 'maximum' 0 = n + 1 \neq n = id n
\]

to see that now the condition \(\text{measPureSpec}\) fails.

**Condition 2.** To exhibit a measure that fails the condition \(\text{measJoinSpec}\), we switch to \(Val = \text{Double}\) and use the arithmetic average

\[
\begin{align*}
\text{avg} : & \text{List Double} \rightarrow \text{Double} \\
\text{avg } [] & = 0.0 \\
\text{avg } ds & = \text{sum } ds / \text{cast (length } ds\text{)}
\end{align*}
\]

as measure \(meas = \text{avg}\). Taking a list of lists of different lengths like \([[1], [2, 3]]\), we have

\[
\begin{align*}
\text{avg } (\text{concat } [[1], [2, 3]]) & = \text{avg } [1, 2, 3] = 2 \\
\neq & \\
\text{avg } (\text{listMap } \text{avg } [[1], [2, 3]]) & = \text{avg } [1, 2.5] = 1.75
\end{align*}
\]

**Condition 3.** Let again \(Val = \mathbb{N}\) to take another look at our counter-example from the last section with \(meas = \text{sum}\), the arithmetic sum of a list. It does fulfil \(\text{measPureSpec}\) and \(\text{measJoinSpec}\), the first by definition, the second by structural induction using the associativity of +. But it fails to fulfil \(\text{measPlusSpec}\). If the list has the form \(a :: as\), we would have to show the following equality for \(\text{measPlusSpec}\) to hold:

\[
(\text{sum} \circ \text{listMap } (v+) ) (a :: as) = ((v+) \circ \text{sum}) (a :: as)
\]

Clearly, if \(v \neq 0\) and \(as \neq []\) this equality cannot hold. This is why in the last section the equality of \(\text{val}\) and \(\text{val'}\) failed for \(meas = \text{sum}\).

However, that the chosen type \(\text{Prob}\) does, e.g. neither enforce that the probabilities lie in the interval \([0, 1]\) nor that they add up to 1. These properties would however be crucial for actual proofs.
A similar failure would arise if we chose \( \text{meas} = \text{foldr} (\ast) 1 \) instead, as \( + \) does not distribute over \( \ast \). But if we turned the situation around by setting \( \oplus = \ast \) and \( \text{meas} = \text{sum} \), the condition \( \text{measPlusSpec} \) would hold thanks to the usual arithmetic distributivity law for \( \ast \) over \( + \).

All of the measures considered in this subsection do fulfill the \( \text{measMonSpec} \) condition imposed by the BJI-theory. This raises the question how previously admissible measures are impacted by adding the three new conditions to the framework.

### 5.2 Impact on previously admissible measures

As we have seen in Section 3.2, the BJI-framework already requires measures to fulfil the monotonicity condition

\[
\text{measMonSpec} : \{ A : \text{Type} \} \rightarrow (f, g : A \rightarrow \text{Val}) \rightarrow ((a : A) \rightarrow (f a) \subseteq (g a)) \rightarrow (ma : MA) \rightarrow \text{meas} (\text{map } f \ ma) \subseteq \text{meas} (\text{map } g \ ma)
\]

Botta et al. show that the arithmetic average (for \( M = \text{List} \)), the worst-case measure (for \( M = \text{List} \) and for a probability monad \( M = \text{Prob} \)) and the expected value measure (for \( M = \text{Prob} \)) all fulfil \( \text{measMonSpec} \). Thus, a natural question is whether these measures also fulfill the three additional requirements.

#### Expected value for probability distributions.

As already discussed, most applications of backward induction concern stochastic SDPs where possible rewards are aggregated using the expected value measure from probability theory, commonly denoted as \( E \).

Essentially, for a numerical type \( Q \), the expected value of a probability distribution on \( Q \) is

\[
E : \text{Num } Q \Rightarrow \text{Prob } Q \rightarrow Q
\]

\[
E pq = \text{sum} \left[ q \ast \text{prob } pq q \mid q \leftarrow \text{supp } pq \right]
\]

where \( \text{prob} \) and \( \text{supp} \) are generic functions that encode the notions of \( \text{probability} \) and of \( \text{support} \) associated with a finite probability distribution:

\[
\text{prob} : \{ A : \text{Type} \} \rightarrow \text{Prob } A \rightarrow A \rightarrow Q
\]

\[
\text{supp} : \{ A : \text{Type} \} \rightarrow \text{Prob } A \rightarrow \text{List } A
\]

For \( pa \) and \( a \) of suitable types, \( \text{prob } pa a \) represents the probability of \( a \) according to \( pa \). Similarly, \( \text{supp } pa \) returns a list of those values whose probability is not zero in \( pa \). The probability function \( \text{prob} \) has to fulfill the axioms of probability theory. In particular,

\[
\text{sum} \left[ \text{prob } pa a \mid a \leftarrow \text{supp } pa \right] = 1
\]

This condition implies that probability distributions cannot be empty, a precondition of \( \text{measPlusSpec} \). Putting forward minimal specifications for \( \text{prob} \) and \( \text{supp} \) is not completely trivial but if the \( + \)-operation associated with \( Q \) is commutative and associative, if \( \ast \) distributes over \( + \) and if the \( \text{map} \) and \( \text{join} \) associated with \( \text{Prob} \) -- for \( f, a, b, pa \) and \( ppa \) of suitable types -- fulfill the conservation law

\[
\text{prob} (\text{map } f \ pa) b = \text{sum } \left[ \text{prob } pa a \mid a \leftarrow \text{supp } pa, f a = b \right]
\]

and the total probability law

\[
\text{prob} (\text{join } ppa) a = \text{sum } \left[ \text{prob } pa a \ast \text{prob } ppa pa \mid pa \leftarrow \text{supp } ppa \right]
\]
then the expected value fulfils \( \text{measPureSpec} \), \( \text{measJoinSpec} \) and \( \text{measPlusSpec} \). This is not surprising since – as stated above – this has been the guiding example for the generalisation to monadic SDPs and the formulation of the three conditions.

**Average and arithmetic sum.** As can already be concluded from the corresponding counter-examples in the previous subsection, neither the plain arithmetic average nor the arithmetic sum are suited as measure when using the standard monad structure on \( \text{List} \) to represent non-deterministic uncertainty. We think this is an important observation, as the average seems innocent enough to come to mind as a simple way to represent uniformly distributed outcomes: “The probability of each element can simply be inferred from the length of the list – so why bother to explicitly deal with probabilities?” Although our counter-example shows that this idea is flawed, the intuition behind it can be employed to define an alternative, but less general monad structure on lists by incorporating the averaging operation into the joining of lists (i.e. by choosing \( \text{join} = \text{map avg} \)). However, this only makes sense for types that are instances of the \( \text{Num} \) and \( \text{Fractional} \) type classes, and naturality only holds for a restricted class of functions (namely additive functions). As a consequence, this alternative structure does not seem particularly useful for our current purpose either.

**Worst-case measures.** In many important applications in climate impact research but also in portfolio management and sports, decisions are taken as to minimise the consequences of worst case outcomes. Depending on how “worse” is defined, the corresponding measures might pick the maximum or minimum from an \( M \)-structure of values. In the previous subsection, we considered an example in which the monad was \( \text{List} \), the operation \( \oplus \) plain addition together with either \( \text{maxList} \) or \( \text{minList} \) as measure. And indeed we can prove that for both measures the three requirements hold (the proofs for \( \text{maxList} \) can be found in the supplementary material). This gives us a useful notion of worst-case measure that is admissible for monadic backward induction.

We can thus conclude that the new requirements hold for certain familiar measures, but that they also rule out certain instances that were considered admissible in the BJI-framework. Given the three conditions \( \text{measPureSpec} \), \( \text{measJoinSpec} \), \( \text{measPlusSpec} \) hold, we can prove the extensional equality of the functions \( \text{val} \) and \( \text{val}' \) generically. This is what we will do in the next section.

### 6 Correctness proofs

In this section, we show that \( \text{val} \) (Section 3.2) and \( \text{val}' \) (Section 4) are extensionally equal

\[
\text{valMeasTotalReward} : \{t, n : \mathbb{N}\} \to (ps : \text{PolicySeq } t \ n) \to (x : X t) \to \text{val}' \ ps \ x = \text{val} \ ps \ x
\]

given the three conditions from the previous section hold. As a corollary, we then obtain our correctness result for monadic backward induction.

We can understand the proof of \( \text{valMeasTotalReward} \) as an optimising program transformation from the less efficient but “obviously correct” implementation \( \text{val}' \) to the more efficient implementation \( \text{val} \). Therefore, the equational reasoning proofs in this section will
proceed from \( val' \) to \( val \). In Section 5, we have stated sufficient conditions for this transformation to be possible: \( measPureSpec \), \( measJoinSpec \), \( measPlusSpec \). We also have seen the different computational patterns that the two implementations exhibit: While \( val' \) first computes all possible trajectories for the given policy sequence and initial state, then computes their individual sum of rewards and finally applies the measure once, \( val \) computes its final result by adding the current reward to an intermediate outcome and applying the measure locally at each decision step. This suggests that a transformation from \( val' \) to \( val \) will essentially have to push the application of the measure into the recursive computation of the sum of rewards. The proof will be carried out by induction on the structure of policy sequences.

### 6.1 Deterministic case

To get a first intuition, let us have a look at what the induction step looks like in the deterministic case (i.e. if we fix monad and measure to be identities):

\[
valMeasTotalReward (p :: ps) x =
\]

\[
(val' (p :: ps) x) = \{ \text{by definition of } val' \} =
\]

\[
(sumR ((x * y) # {trj ps x'})') = \{ \text{by definition of } sumR \} =
\]

\[
(r (head (trj ps x')) \oplus val' ps x') = \{ \text{by headLemma} \} =
\]

\[
(r x' \oplus val' ps x') = \{ \text{by induction hypothesis} \} =
\]

\[
(r x' \oplus val ps x') = \{ \text{by definition of } val \} =
\]

\[
(val (p :: ps) x) \square
\]

where \( y = p x, x' = next t x y \) and \( r = reward t x y \). In the proof sketch, we have first applied the definitions of \( val' \) and \( sumR \). Using the fact that in the deterministic case \( trj \) returns exactly one state-control sequence and that the \textit{head} of any trajectory starting in \( x' \) is just \( x' \) (let us call the latter \textit{headLemma}), the left-hand side of the sum simplifies to \( rx' \). Its right-hand side amounts to \( val' ps x' \) so that we can apply the induction hypothesis. The rest of the proof only relies on definitional equalities. Thus in the deterministic case \( val \) and \( val' \) are unconditionally extensionally equal – or rather, the conditions of Section 5 are trivially fulfilled.

### 6.2 Lemmas

To prove the general, monadic case, we proceed similarly. This time, however, the situation is complicated by the presence of the abstract monad \( M \). Instead of being able to use the type structure of some concrete monad, we need to leverage on the properties of \( M, meas \) and \( \oplus \) postulated in Section 5. To facilitate the main proof, we first prove three lemmas about the interaction of the measure with the monad structure and the \( \oplus \)-operator on \( Val \). Machine-checked proofs are given in the Appendices 2, 3 and 4. The monad laws we use are stated in Appendix 1.2. In the remainder of this section, we discuss semi-formal versions of the proofs.
Monad algebras. The first lemma allows us to lift and eliminate an application of the monad’s \texttt{join} operation:

\[
\text{measAlgLemma} : \{ A : B \rightarrow \text{Type} \} \rightarrow (f : B \rightarrow \text{Val}) \rightarrow (g : A \rightarrow M B) \rightarrow \\
(\text{meas} \circ \text{map} (\text{meas} \circ \text{map} f \circ g)) = (\text{meas} \circ \text{map} f \circ \text{join} \circ \text{map} g)
\]

The proof of this lemma hinges on the condition \texttt{measJoinSpec}. It allows to trade the application of \texttt{join} against an application of \texttt{map meas}. The rest is just standard reasoning with monad and functor laws, i.e. we use that the functorial map for \texttt{M} preserves composition and that \texttt{join} is a natural transformation:

\[
\text{measAlgLemma} f g ma = \\
(\text{meas} \circ \text{map} (\text{meas} \circ \text{map} f \circ g)) ma = \{\text{map preserves composition}\} = \\
(\text{meas} \circ \text{map} (\text{meas} \circ \text{map} f) \circ \text{map} g) ma = \{\text{map preserves composition}\} = \\
(\text{meas} \circ \text{join} \circ \text{map} (\text{map} f) \circ \text{map} g) ma = \{\text{join is a natural transformation}\} = \\
(\text{meas} \circ \text{map} f \circ \text{join} \circ \text{map} g) ma
\]

This lemma is generic in the sense that it holds for arbitrary Eilenberg–Moore algebras of a monad. Here we prove it for the framework’s measure \texttt{meas}, but note that in the appendix, we prove a generic version that is then appropriately instantiated.

Head/trajectory interaction. The second lemma amounts to a lifted version of \texttt{headLemma} in the deterministic case. Mapping \texttt{head} onto an \texttt{M}-structure of trajectories computed with \texttt{trj} results in an \texttt{M}-structure filled with the initial states of these trajectories; similarly, mapping \((r \circ \texttt{head} \bigoplus s)\) onto \texttt{trj ps x} for functions \texttt{s} and \texttt{r} of appropriate type is the same as mapping \((\texttt{const} (r x) \bigoplus s)\) onto \texttt{trj ps x} (where \texttt{const} is the constant function). We can prove

\[
\text{headTrjLemma} : \{ t, n : \mathbb{N} \} \rightarrow (ps : \text{PolicySeq} t n) \rightarrow (r : X t \rightarrow \text{Val}) \rightarrow \\
(s : \text{StateCtrlSeq} t (S n) \rightarrow \text{Val}) \rightarrow (x : X t) \rightarrow \\
(\text{map} (r \circ \texttt{head} \bigoplus s) \circ \texttt{trj ps}) x = \\
(\text{map} (\texttt{const} (r x) \bigoplus s) \circ \texttt{trj ps}) x
\]

by doing a case split on \texttt{ps}. In case \texttt{ps} = \texttt{Nil}, the equality holds because the monad’s \texttt{pure} is a natural transformation and in case \texttt{ps} = \texttt{p :: ps’} because \texttt{M}’s functorial \texttt{map} preserves composition.

Measure/sum interaction. The third lemma allows us to both commute the measure into the right summand of an \bigoplus-sum and to perform the head/trajectory simplification. It lies at the core of the relationship between \texttt{val} and \texttt{val’}.

\[
\text{measSumLemma} : \{ t, n : \mathbb{N} \} \rightarrow (ps : \text{PolicySeq} t n) \rightarrow \\
(r : X t \rightarrow \text{Val}) \rightarrow \\
(s : \text{StateCtrlSeq} t (S n) \rightarrow \text{Val}) \rightarrow \\
(\text{meas} \circ \text{map} (r \circ \texttt{head} \bigoplus s) \circ \texttt{trj ps}) = \\
(r \bigoplus \text{meas} \circ \text{map} s \circ \texttt{trj ps})
\]

Recall that our third condition from Section 5, \texttt{measPlusSpec}, plays the role of a distributive law and allows us to “factor out” a partially applied sum \((v \bigoplus)\) for arbitrary \(v : \text{Val}\). Given that \texttt{measPlusSpec} holds, the lemma is provable by simple equational reasoning using the above head-trajectory lemma and the fact that map preserves composition:
measSumLemma ps r s x' =

((meas o map (r o head s) o trj ps) x') =\{ by headTrjLemma \}=
((meas o map (const (r') s) o trj ps) x') =\{ by definition of s, o \}=
((meas o map ((const (r') id) s) o trj ps) x') =\{ map preserves composition \}=
((meas o map (const (r') id) o map s o trj ps) x') =\{ by definition of meaPlusSpec \}=
(((r'+) o meas o map s o trj ps) x') =\{ by definition of (r') \}=
((r meas o map s o trj ps) x')

□

Notice how measPlusSpec is used to transform an application of meas o map ((r')+) into an application of ((r')+) o meas. This is essential to simplify the computation of the measured total reward: instead of first adding the current reward to the intermediate outcome of each individual trajectory and then measuring the outcomes, one can first measure the intermediate outcomes of the trajectories and then add the current reward.

6.3 Correctness of the BJI-value function

With the above lemmas in place, we now prove that val is extensionally equal to val'.

Let t, n : N, ps : PolicySeq t n. We prove valMeasTotalReward by induction on ps.

Base case. We need to show that for all x : X t, val' Nil x = val Nil x. The right-hand side of this equation reduces to zero by definition. The left-hand side can be simplified to meas (pure zero) since pure is a natural transformation. At this point, our first condition, measPureSpec, comes into play: Using that meas is inverse to pure on the left, we can conclude that the equality holds.

In equational reasoning style: For all x : X t,

valMeasTotalReward Nil x =

(val' Nil x) =\{ by definition of val' \}=
(meas (map sumR (trj Nil x))) =\{ by definition of trj \}=
(meas (map sumR (pure (Last x)))) =\{ pure is a natural transformation \}=
(meas (pure (sumR (Last x)))) =\{ by definition of sumR \}=
(meas (pure zero)) =\{ by measPureSpec \}=
(zero) =\{ by definition of val \}=
(val Nil x)

Step case. The induction hypothesis (IH) is: for all x : X t, val' ps x = val ps x. We have to show that IH implies that for all p : Policy t and x : X t, the equality val' (p :: ps) x = val (p :: ps) x holds.

For brevity (and to economise on brackets), let in the following y = px, mx' = next t xy, r = reward t xy, trjps = trj ps, and consxy = ((x ** y)#).
As in the base case, all that has to be done on the \textit{val}-side of the equation only depends on definitional equality. However, it is more involved to bring the \textit{val}'-side into a form in which the induction hypothesis can be applied. This is where we leverage on the lemmas proved above.

By definition and because \textit{map} preserves composition, we know that \( \textit{val}'(p :: ps)x \) is equal to \((\textit{meas} \circ \textit{map} ((r \circ \textit{head}) \oplus \textit{sumR}) (\textit{mx}' \gg \textit{trjps})\). We use the relation between the monad’s \textit{bind} and \textit{join} to eliminate the \textit{bind}-operator from the term. Now we can apply the first lemma from above, \textit{measAlgLemma}, to lift and eliminate the \textit{join} operation.

To commute the measure under the \(\oplus\) and get rid of the application of \textit{head}, we use our third lemma, \textit{measSumLemma}. At this point, we can apply the induction hypothesis and the resulting term is equal to \(\textit{val} \, \textit{ps} \, x\) by definition.

The more detailed equational reasoning proof:

\[
\text{valMeasTotalReward} \, (p :: ps) \, x =

\begin{align*}
(\text{val}' \, (p :: ps) \, x) &= \quad \text{=} \quad \text{by definition of \textit{val}'} \\
(\text{meas} \, (\text{map} \, \text{sumR} \, (\text{trj} \, (p :: ps) \, x))) &= \quad \text{=} \quad \text{by definition of \textit{trj}} \\
(\text{meas} \, (\text{map} \, \text{sumR} \, (\text{map} \, \text{consxy} \, (\text{mx}' >\gg \textit{trjps}))) &= \quad \text{=} \quad \text{map preserves composition} \\
(\text{meas} \, (\text{map} \,(r \circ \textit{head}) \oplus \textit{sumR})\,(\text{mx}' >\gg \textit{trjps}))) &= \quad \text{=} \quad \text{by definition of \textit{sumR}} \\
(\text{meas} \,(\text{map} \, ((r \circ \textit{head}) \oplus \textit{sumR}) \, (\textit{join} \, (\text{map} \, \text{trjps} \, \text{mx}'))) &= \quad \text{=} \quad \text{by \textit{measAlgLemma}} \\
(\text{meas} \, (\text{map} \, (r \circ \textit{head}) \oplus \textit{sumR}) \, \textit{join} \, (\text{map} \, \text{trjps} \, \text{mx}')) &= \quad \text{=} \quad \text{by \textit{measSumLemma}} \\
(\text{meas} \, (\text{map} \, (r \oplus \textit{meas} \, \text{map} \, \textit{sumR} \, \textit{join} \, (\text{map} \, \text{trjps} \, \text{mx}'))) &= \quad \text{=} \quad \text{by definition of \textit{val}'} \\
(\text{meas} \, (\text{map} \, (r \oplus \textit{meas} \, \text{map} \, \textit{sumR} \, \textit{trjps}) \, \text{mx}')) &= \quad \text{=} \quad \text{by \textit{induction hypothesis}} \\
(\text{meas} \, (\text{map} \, (r \oplus \textit{val} \, \textit{ps}) \, \text{mx}')) &= \quad \text{=} \quad \text{by definition of \textit{val}} \\
(\text{val} \, (p :: ps) \, x) &= \quad \text{=} \quad \text{by definition of \textit{val}}
\end{align*}
\]

\[
\square
\]

\textbf{Technical remarks.} The above proof of \textit{valMeasTotalReward} oms some technical details that may be uninteresting for a pen and paper proof, but turn out to be crucial in the setting of an intensional type theory – like Idris – where function extensionality does not hold in general. In particular, we have to postulate that the functorial \textit{map} preserves extensional equality (see Appendix 1.2 and Botta et al. (n.d.)) for Idris to accept the proof. In fact, most of the reasoning proceeds by replacing functions that are mapped onto monadic values by other functions that are only extensionally equal. Using that \textit{map} preserves extensional equality allows to carry out such proofs generically without knowledge of the concrete structure of the functor.

\subsection*{6.4 Correctness of monadic backward induction}

As corollary, we can now prove the correctness of monadic backward induction, namely that the policy sequences computed by \textit{bi} are optimal with respect to the measured total reward computed by \textit{val}':

\[
\text{biOptMeasTotalReward} : (t, n : \mathbb{N}) \rightarrow \text{GenOptPolicySeq} \, \textit{val}' \, (\textit{bi} \, t \, n)
\]

\begin{footnote}
\footnotesize
We are very grateful to the anonymous reviewer who suggested an alternative proof for the induction step. The proof presented here is based on his proof, and his suggestions have lead to significantly weaker conditions on the measure and thus a stronger result.
\end{footnote}
biOptMeasTotalReward t n ps' x =
let vvEqL = sym (valMeasTotalReward ps' x) in
let vvEqR = sym (valMeasTotalReward (bi t n) x) in
let biOpt = biOptVal t n ps' x in
replace vvEqR (replace vvEqL biOpt)

7 Discussion

In the last two sections, we have seen what the three conditions mean for concrete examples and how they are used in the correctness proof. In this section, we take a step back and consider them from a more abstract point of view.

Category-theoretical perspective. Readers familiar with the theory of monads might have recognised that the first two conditions ensure that meas is the structure map of a monad algebra for $M$ on $Val$ and thus the pair $(Val, meas)$ is an object of the Eilenberg–Moore category associated with the monad $M$. The third condition requires the map $(v \oplus)$ to be an $M$-algebra homomorphism – a structure preserving map – for arbitrary values $v$.

This perspective allows us to use existing knowledge about monad algebras as a first criterion for choosing measures. For example, the Eilenberg–Moore algebras of the list monad are monoids – this implicitly played a role in the examples we considered above. Jacobs (2011) shows that the algebras of the distribution monad for probability distributions with finite support correspond to convex sets. Interestingly, convex sets play an important role in the theory of optimal control (Bertsekas et al., 2003).

Measures for the list monad. The knowledge that monoids are List-algebras suggests a generic description of admissible measures for $M = List$: Given a monoid $(Val, \odot, b)$, we can prove that monoid homomorphisms of the form $foldr \odot b$ fulfil the three conditions, if $\oplus$ distributes over $\odot$ on the left. I.e. for $meas = foldr \odot b$ the three conditions can be proven from

\[
\begin{align*}
odotNeutrRight &: (l : Val) \to l \odot neutr = l \\
odotNeutrLeft &: (r : Val) \to neutr \odot r = r \\
odotAssociative &: (l, v, r : Val) \to l \odot (v \odot r) = (l \odot v) \odot r \\
oplusOdotDistrLeft &: (n, l, r : Val) \to n \oplus (l \odot r) = (n \oplus l) \odot (n \oplus r)
\end{align*}
\]

Neutrality of $b$ on the right is needed for $measPureSpec$, while $measJoinSpec$ follows from neutrality on the left and the associativity of $\odot$. The algebra morphism condition on $(v \oplus)$ is provable from the distributivity of $\oplus$ over $\odot$ and again neutrality of $b$ on the right. If moreover $\odot$ is monotone with respect to $\sqsubseteq$

\[
\text{odotMon} : \{a, b, c, d : Val\} \to a \sqsubseteq b \to c \sqsubseteq d \to (a \odot c) \sqsubseteq (b \odot d)
\]

then we can also prove $measMonSpec$ using the transitivity of $\sqsubseteq$. The proofs are simple and can be found in the supplementary material to this paper. This also illustrates how the three abstract conditions follow from more familiar algebraic properties.

Mutual independence. Although it does not seem surprising, it should be noted that the three conditions are mutually independent. This can be concluded from the
counter-examples in Section 5.1: The sum, the modified list maximum and the arithmetic average each fail exactly one of the three conditions.

**Sufficient versus necessary.** The three conditions are sufficient to prove the extensional equality of the functions val and val’. They are justified by their level of generality and the fact that they hold for standard measures used in control theory. However, we leave open the interesting question whether these conditions are also necessary for the correctness of monadic backward induction.

**Non-emptiness requirement.** Note that mv in the premises of measPlusSpec is required to be non-empty. This condition arises from a pragmatic consideration. As an example, let us again use the list monad with Val = N and ⊕ = +. It is not hard to see that for any natural number n greater than 0 the equality meas(map(n+)[]) = n + meas[] must fail. So, if we wish to use the standard list data type instead of defining a custom type of non-empty lists, the only way to prove the base case of measPlusSpec is by contradiction with the non-emptiness premise.

However, omitting the premise mv: NotEmpty would not prevent us from generically proving the correctness result of Section 6 – it would even simplify matters as it would spare us reasoning about preservation of non-emptiness. But it would implicitly restrict the class of monads that can be used to instantiate M. For example, we have seen above that measPlusSpec is not provable for the empty list without the non-emptiness premise and we would therefore need to resort to a custom type of non-empty lists instead.

The price to pay for including the non-emptiness premise is the additional condition nextNotEmpty on the transition function next that was already stated in Section 3.3. Moreover, we have to postulate non-emptiness preservation laws for the monad operations (Appendix 1.2) and to prove an additional lemma about the preservation of non-emptiness (Appendix 4). Conceptually, it might seem cleaner to omit the non-emptiness condition: In this case, the remaining conditions would only concern the interaction between the monad, the measure, the type of values and the binary operation ⊕. However, the non-emptiness preservation laws seem less restrictive with respect to the monad. In particular, for our above example of ordinary lists they hold (the relevant proofs can be found in the supplementary material). Thus, we have opted for explicitly restricting the next function instead of implicitly restricting the class of monads for which the result of Section 6 holds.

### 8 Conclusion

In this paper, we have proposed correctness criteria for monadic backward induction and its underlying value function in the framework for specifying and solving finite-horizon, monadic SDPs proposed in Botta et al. (2017a). After having shown that these criteria are not necessarily met for arbitrary monadic SDPs, we have formulated three general compatibility conditions. We have given a proof that monadic backward induction and its underlying value function are correct if these conditions are fulfilled.

The main theorem has been proved via the extensional equality of two functions: (1) the value function of Bellman’s dynamic programming (Bellman, 1957) and optimal control
theory (Bertsekas, 1995; Puterman, 2014) that is also at the core of the generic backward induction algorithm of Botta et al. (2017a) and (2) the measured total reward function that specifies the objective of decision making in monadic SDPs: the maximisation of a measure of the sum of the rewards along the trajectories rooted at the state associated with the first decision.

Our contribution to verified optimal decision making is twofold: On the one hand, we have implemented a machine-checked generalisation of the semi-formal results for deterministic and stochastic SDPs discussed in Bertsekas (1995, Prop. 1.3.1) and Puterman (2014, Theorem 4.5.1.c). As a consequence, we now have a provably correct method for solving deterministic and stochastic sequential decision problems with their canonical measure functions. On the other hand, we have identified three general conditions that are sufficient for the equivalence between the two functions and thus the correctness result to hold. The first two conditions are natural compatibility conditions between the measure of uncertainty \( \text{meas} \) and the monadic operations associated with the uncertainty monad \( M \). The third condition is a distributivity principle concerning the relationship between \( \text{meas} \), the functorial map associated with \( M \) and the rule for adding rewards \( \oplus \). All three conditions have a straightforward category-theoretical interpretation in terms of Eilenberg-Moore algebras (MacLane, 1978, ch. VI.2). As discussed in Section 7, the three conditions are independent and have non-trivial implications for the measure and the addition function that cannot be derived from the monotonicity condition on \( \text{meas} \) already imposed in Ionescu (2009); Botta et al. (2017a).

A consequence of this contribution is more flexibility: We can now compute verified solutions of stochastic sequential decision problems in which the measure of uncertainty is different from the expected value measure. This is important for applications in which the goal of decision making is, for example, of maximising the value of worst-case outcomes. To the best of our knowledge, the formulation of the compatibility condition and the proof of the equivalence between the two value functions are novel results.

The latter can be employed in a wider context than the one that has motivated our study: in many practical problems in science and engineering, the computation of optimal policies via backward induction (let apart brute-force or gradient methods) is simply not feasible. In these problems one often still needs to generate, evaluate and compare different policies and our result shows under which conditions such evaluation can safely be done via the “fast” value function \( \text{val} \) of standard control theory.

Finally, our contribution is an application of verified, literal programming to optimal decision making: the sources of this document have been written in literal Idris and are available at Brede & Botta (2021), where the reader can also find the bare code and some examples. Although the development has been carried out in Idris, it should be readily reproducible in other implementations of type theory like Agda or Coq.

**Acknowledgements**

The work presented in this paper was motivated by a remark of Marina Martínez Montero who raised the question of the equivalence between \( \text{val} \) and \( \text{val}' \) (and, thus, of the correctness of the Botta et al. framework) during an introduction to verified decision making that...
the authors gave at UCL (Université catholique de Louvain) in 2019. We are especially thankful to Marina for that question!

We are grateful to Jeremy Gibbons, Christoph Kreitz, Patrik Jansson, Tim Richter and to the JFP editors and reviewers, whose comments and recommendations have lead to significant improvements of the original manuscript.

A very special thanks goes to the anonymous reviewer who has suggested both a more straightforward proof of the $val$-$val'$ equality and, crucially, weaker conditions on the measure function for the result to hold. This warrants the applicability of the Botta et al. framework for verified decision making to a wider class of problems than our original conditions.

The work presented in this paper heavily relies on free software, among others on Coq, Idris, Agda, GHC, git, vi, Emacs, LATEX and on the FreeBSD and Debian GNU/Linux operating systems. It is our pleasure to thank all developers of these excellent products. This is TiPES contribution No 37. This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 820970 (TiPES – Tipping Points in the Earth System, 2019–2023).

Conflicts of interest

None.

Supplementary material

For supplementary material for this article, please visit http://dx.doi.org/10.1017/S0956796821000228.

References


**Appendices**

### 1 Preliminaries

#### 1.1 General remarks concerning the Idris formalisation

- Idris’ type checker often struggles with dependencies in implicit arguments. We sometimes use abbreviations to avoid cluttering the proofs with implicit arguments.
- As a standard, we write \((f \circ g \circ h)\) instead of \(f(g(h(x)))\).
  - When this is a problem for the type checker, we use the second notation.
- Functions that are not defined explicitly are from the Idris standard library. Examples are *cong, void* and *concat*. 

Downloaded from [https://www.cambridge.org/core](https://www.cambridge.org/core). Bibliothek des Wissenschaftsparks Albert Einstein, on 26 Nov 2021 at 12:43:29, subject to the Cambridge Core terms of use, available at [https://www.cambridge.org/core/terms](https://www.cambridge.org/core/terms). https://doi.org/10.1017/S0956796821000228
• Proofs in Idris can be implemented by preorder reasoning. I.e. equational reasoning steps of the form

\[(t_1) \equiv [\text{step}] = (t_2)\]

as displayed in this appendix are actual type-checkable implementations of proofs.

### 1.2 Monad laws

In the BJI-framework, \( M \) is required to be a container monad but none of the standard monad laws (Bird, 2014) is required for the verification result to hold. By contrast, to prove our extended correctness result, we need \( M \) to be a full-fledged monad. More specifically, we require of the monad \( M \) that

- it is equipped with functor and monad operations:
  
  \[
  \begin{align*}
  \text{map} & : \{A, B : \text{Type}\} \to (A \to B) \to MA \to MB \\
  \text{pure} & : \{A : \text{Type}\} \to A \to MA \\
  \text{bind} & : \{A, B : \text{Type}\} \to MA \to (A \to M B) \to MB
  \end{align*}
  \]

- it preserves extensional equality (Botta et al., n.d.), identity and composition of arrows:

  \[
  \begin{align*}
  \text{mapPresEE} & : \{A, B : \text{Type}\} \to (f, g : A \to B) \to f \equiv g \to \text{map } f \equiv \text{map } g \\
  \text{mapPresId} & : \{A : \text{Type}\} \to \text{map } id \equiv id \\
  \text{mapPresComp} & : \{A, B, C : \text{Type}\} \to (f : A \to B) \to (g : B \to C) \to \\
  \text{map } (g \circ f) & \equiv \text{map } g \circ \text{map } f
  \end{align*}
  \]

- Its pure and join operations are natural transformations (see MacLane, 1978, 1.4):

  \[
  \begin{align*}
  \text{pureNatTrans} & : \{A, B : \text{Type}\} \to (f : A \to B) \to \text{map } f \circ \text{pure} \equiv \text{pure } \circ f \\
  \text{joinNatTrans} & : \{A, B : \text{Type}\} \to (f : A \to B) \to \text{map } f \circ \text{join} \equiv \text{join } \circ \text{map } (\text{map } f)
  \end{align*}
  \]

and fulfil the neutrality and associativity axioms:

\[
\begin{align*}
\text{pureNeutralLeft} & : \{A : \text{Type}\} \to \text{join } \circ \text{pure} \equiv \text{id} \\
\text{pureNeutralRight} & : \{A : \text{Type}\} \to \text{join } \circ \text{map } \text{pure} \equiv \text{id} \\
\text{joinAssoc} & : \{A : \text{Type}\} \to \text{join } \circ \text{map } \text{join} \equiv \text{join } \circ \text{join}
\end{align*}
\]

Notice that the above specification of the monad operations is not minimal: \((\gg\gg)\) is not assumed to be implemented in terms of \(\text{join}\) and \(\text{map}\) (or \(\text{map}\) and \(\text{join}\) via \((\gg\gg)\) and \(\text{pure}\)). Therefore, \((\gg\gg)\) (pronounced “bind”), \(\text{join}\) and \(\text{map}\) have to fulfil:

\[
\text{bindJoinSpec} : \{A, B : \text{Type}\} \to (ma : MA) \to (f : A \to M B) \to (ma \gg\gg f) = \text{join } (\text{map } f \text{ ma})
\]

The equality in the axioms is extensional equality, not the type theory’s definitional equality:

\[
\begin{align*}
(\equiv) : \{A, B : \text{Type}\} \to (f, g : A \to B) \to \text{Type} \\
(\equiv) & : \{A\} \to f g = (a : A) \to f a = g a
\end{align*}
\]
As Idris does not have function extensionality, not postulating definitional equalities makes the axioms strictly weaker. The BJI-framework also requires $M$ to be equipped with type-level membership, with a universal quantifier and with a type-valued predicate

$\text{NotEmpty} : \{A : \text{Type}\} \to MA \to \text{Type}$

For our purposes, the monad operations are moreover required to fulfil the following preservation laws:

- The $M$-structure obtained from lifting an element into the monad is not empty:

  $\text{pureNotEmpty} : \{A : \text{Type}\} \to (a : A) \to \text{NotEmpty} (\text{pure } a)$

- The monad’s $\text{map}$ and $\text{bind}$ preserve non-emptiness:

  $\text{mapPresNotEmpty} : \{A, B : \text{Type}\} \to (f : A \to B) \to (ma : MA) \to \text{NotEmpty } ma \to \text{NotEmpty } (\text{map } f \text{ } ma)$

  $\text{bindPresNotEmpty} : \{A, B : \text{Type}\} \to (f : A \to MB) \to (ma : MA) \to \text{NotEmpty } ma \to (a : A) \to \text{NotEmpty } (f \text{ } a) \to \text{NotEmpty } (ma \gg= f)$

As discussed in Section 7, we could have omitted these non-emptiness preservation laws, but instead would have implicitly restricted the class of monads for which the correctness result holds.

### 1.3 Preservation of extensional equality

We have stated above that for our correctness proof the functor $M$ has to satisfy the monad laws and moreover its functorial $\text{map}$ has to preserve extensional equality.

This e.g. is the case for $M = \text{Identity}$ (no uncertainty), $M = \text{List}$ (non-deterministic uncertainty) and for the finite probability distributions (stochastic uncertainty, $M = \text{Prob}$) discussed in Botta et al. (2017a). For $M = \text{List}$ the proof of $\text{mapPresEE}$ amounts to:

\[
\text{mapPresEE} : \{A, B : \text{Type}\} \to (f, g : A \to B) \to f \triangleq g \to \text{map } f \triangleq \text{map } g
\]

\[
\text{mapPresEE } f \ g \ p \ \text{Nil} = \text{Refl}
\]

\[
\text{mapPresEE } f \ g \ p (a :: as) =
\]

\[
(\text{map } f (a :: as)) = \text{Refl} \}
\]

\[
\text{cong }\{f = \lambda x \Rightarrow x :: \text{map } f \text { } as\}(p \ a) =
\]

\[
\text{cong } (\text{mapPresEE } f \ g \ p \ as) =
\]

\[
\text{cong } (g a :: \text{map } g \text { } as) = \text{Refl} \}
\]

\[
(\text{map } g (a :: as)) = \]

\[
\square
\]

The principle of extensional equality preservation is discussed in more detail in Botta et al. (n.d.).

### 2 Correctness of the value function

\[
\text{valMeasTotalReward} : \{t, n : \mathbb{N}\} \to (ps : \text{PolicySeq } t \ n) \to (x : X \ t) \to \text{val}'ps \ x = \text{val} \ ps \ x
\]
valMeasTotalReward Nil x =
(val' Nil x) =| Refl |
(meas (map sumR (trj Nil x))) =| Refl |
(meas (map sumR (pure (Last x)))) =| cong (pureNatTrans sumR (Last x)) |
(meas (pure (sumR (Last x)))) =| Refl |
(meas (pure zero)) =| measPureSpec zero |
(zero) =| Refl |
(val Nil x)

valMeasTotalReward { t } { n = S m } (p :: ps) x =
  -- type abbreviations
  let SCS  : Type = StateCtrlSeq (S t) (S m) in
  let SCS' : Type = StateCtrlSeq t (S (S m)) in

  -- element and function abbreviations
  let y    : Y tx = p x in
  let mx'  : M (X (S t)) = next tx y in
  let r    : (X (S t) → Val) = reward tx y in
  let trjps : (X (S t) → M SCS) = trj ps in
  let consxy : (SCS → SCS') = ((x ** y)@)# in
  let mx'trips : M SCS = (mx' ⊕ trjps) in
  let sR   : (SCS → Val) = sumR { t = S t } { n = S m } in
  let hd   : (SCS → X (S t)) = head { t = S t } { n = m } in

  -- proof steps:
  let useMapPresComp = mapPresComp consxy sumR mx'trips in
  let useBindJoinSpec = bindJoinSpec { B = SCS } trjps mx' in
  let useAlgLemma = algLemma { B = SCS } meas measJoinSpec
                   ((r ∘ hd) ⊕ sumR) trjps mx' in
  let useMeasSumLemma = mapPresEE
                         (meas ∘ map (r ∘ hd ⊕ sR) ∘ trjps)
                         (r ⊕ meas ∘ map sR ∘ trjps)
                         (measSumLemma ps r sR)
                         mx' in
  let useIH = mapPresEE
              (r ⊕ val' ps)
              (r ⊕ val ps)
              (oplusLiftEERight (val' ps)
                           (val ps) r (valMeasTotalReward ps))
              mx' in
  let ctx = λa → meas ∘ map ((r ∘ hd) ⊕ sumR) a in
  (val' (p :: ps) x) =| Refl |
  (meas (map sumR (trj (p :: ps) x))) =| Refl |
  (meas (map sumR (map consxy mx'trips))) =| cong (sym useMapPresComp) |
  (meas (map (sumR ∘ consxy) mx'trips)) =| Refl |
  (meas (map ((r ∘ hd) ⊕ sR) mx'trips)) =| cong { f = ctx } useBindJoinSpec |
  (meas (map (map (meas ∘ map (r ∘ hd ⊕ sR) ∘ trjps) mx')) =| sym useAlgLemma |
  (meas (map (r ⊕ meas ∘ map sR ∘ trjps) mx')) =| Refl |
3 Correctness of monadic backward induction

Together with the result of Botta et al. (biOptVal, see Appendix 6 below), we can prove the correctness of monadic backward induction as corollary, using a generalised optimality of policy sequences predicate:

\[
\text{GenOptPolicySeq : } \{ t, n : \mathbb{N} \} \rightarrow (f : \text{PolicySeq } t n \rightarrow X t \rightarrow \text{Val}) \rightarrow \text{PolicySeq } t n \rightarrow \text{Type}
\]

\[
\text{GenOptPolicySeq } \{ t \} \{ n \} f ps = (ps' : \text{PolicySeq } t n) \rightarrow (x : X t) \rightarrow f \overset{\text{ps' } x}{\rightarrow} f \overset{\text{ps } x}{\rightarrow}
\]

\[
\text{biOptMeasTotalReward : } \{ t : \mathbb{N} \} \rightarrow (n : \mathbb{N}) \rightarrow \text{GenOptPolicySeq } val' \{ bi t n \}
\]

\[
\text{biOptMeasTotalReward } t n ps' x =
\]

\[
\text{let } vvEqL = \text{sym} (\text{valMeasTotalReward } ps' x) \text{ in } -- val' ps' x = val ps' x
\]

\[
\text{let } vvEqR = \text{sym} (\text{valMeasTotalReward } (bi t n) x) \text{ in } -- val' (bi t n) x = val (bi t n) x
\]

\[
\text{let } biOpt = \text{biOptVal } t n ps' x \text{ in } -- val ps' x \subseteq val (bi t n) x
\]

\[
\text{let } lP = \lambda v \Rightarrow v \subseteq \text{val } (bi t n) x \text{ in }
\]

\[
\text{let } rP = \lambda v \Rightarrow val' ps' x \subseteq v \text{ in }
\]

\[
\text{replace } \{ P = rP \} vvEqR (\text{replace } \{ P = lP \} vvEqL biOpt)
\]

4 Lemmas

The proof of valMeasTotalReward relies on a few auxiliary results which we prove here.

Lemma about the interaction of head and trj interleaved with map:

\[
\text{headTrjLemma : } \{ t, n : \mathbb{N} \} \rightarrow (ps : \text{PolicySeq } t n) \rightarrow (r : X t \rightarrow \text{Val}) \rightarrow (s : \text{StateCtrlSeq } t (S n) \rightarrow \text{Val}) \rightarrow (x' : X t) \rightarrow (map (r \circ \text{head } \oplus s) \circ \text{trj } ps) x' = (map (\text{const } (r x') \oplus s) \circ \text{trj } ps) x'
\]

\[
\text{headTrjLemma } \{ t \} \{ n = Z \} \text{Nil } r s x' =
\]

\[
\text{let } hd = \text{head } \{ t \} \text{ in }
\]

\[
\text{let } lastx' = \text{Last } \{ t \} x' \text{ in }
\]

\[
\text{let } nil = \text{Nil } \{ t \} \text{ in }
\]

\[
\text{let } \text{usePureNatTrans } = \text{pureNatTrans } (r \circ \text{hd } \oplus s) \text{ lastx'} \text{ in }
\]

\[
\text{let } \text{usePureNatTransSym } = \text{sym } (\text{pureNatTrans } ((\oplus) (r x') \circ s) \text{ lastx'}) \text{ in }
\]

\[
\begin{align*}
\text{((map } & (r \circ \text{hd } \oplus s)) (\text{trj } nil x')) \Rightarrow \text{Refl} = \\
\text{((map } & (r \circ \text{hd } \oplus s)) (\text{pure lastx'}) \Rightarrow \text{usePureNatTrans } = \\
\text{(pure } & (r \circ \text{hd } \oplus s) \text{ lastx'}) \Rightarrow \text{Refl} = \\
\text{(pure } & (\text{const } (r x') \oplus s) \text{ lastx'}) \Rightarrow \text{usePureNatTransSym } = \\
\text{(map } & (\text{const } (r x') \oplus s) \text{ lastx'}) \Rightarrow \text{Refl} = \\
\text{(map } & (\text{const } (r x') \oplus s) (\text{trj } nil x')) \Rightarrow \\
\end{align*}
\]

\[
\text{headTrjLemma } \{ t = t \} \{ n = S n \} (p :: ps) r s x' =
\]

\[
\text{let } y' = p x' \text{ in }
\]
Lemma about the commutation of $\text{meas} \circ \text{map}$ and $\oplus$:

$\text{measSumLemma}: \{t, n : \mathbb{N}\} \rightarrow (ps : \text{PolicySeq } t n) \rightarrow$
$$ (r : X \rightarrow \text{Val}) \rightarrow$$
$$ (s : \text{StateCtrlSeq } t (S n) \rightarrow \text{Val}) \rightarrow$$
$$ (\text{meas} \circ \text{map} (r \circ \text{head} \oplus s) \circ \text{trj } ps) =$$
$$ (r \oplus \text{meas} \circ \text{map} s \circ \text{trj } ps)$$

Non-emptiness proofs:

Let $\text{trjNE} = \text{trjNotEmptyLemma } ps x'$

Proof steps:

Let $\text{useMapPresComp} = \text{mapPresComp } \text{conx} x' (\text{const } (r x') \oplus s) mx''$trips

Let $\text{useMapPresCompSym} = \text{sym } (\text{mapPresComp } \text{conx} x' (r \circ \text{head} \oplus s) mx''$trips)

((map $ (r \circ \text{head} \oplus s) \circ \text{trj } ps$) $x)$

\[ \Rightarrow \text{Refl} \]

((map $ (r \circ \text{head} \oplus s) \circ \text{map} \text{conx} x'$) $mx''$trips)

\[ \Rightarrow \text{useMapPresComp} \]

((map $ ((\text{const } (r x') \oplus s) \circ \text{conx} x') mx''$trips)

\[ \Rightarrow \text{Refl} \]

((map $ (\text{const } (r x') \oplus s) (\text{map} \text{conx} x' mx''$trips))

\[ \Rightarrow \text{Refl} \]

Lemma about the commutation of $\text{meas} \circ \text{map}$ and $\oplus$:

The $\text{trj}$ function never produces an empty $M$-structure of trajectories:

$\text{trjNotEmptyLemma} : \{t, n : \mathbb{N}\} \rightarrow (ps : \text{PolicySeq } t n) \rightarrow (x : X \rightarrow \text{Val}) \rightarrow \text{NotEmpty } (\text{trj } ps\ x)$

$\text{trjNotEmptyLemma} \left(\text{Nil} \right) x = \text{pureNotEmpty } (\text{Last } x)$

$\text{trjNotEmptyLemma} \left( \left\{ t = t \right\} \right) n \left\{ p :: ps \right\} x =$
A technical lemma to lift equalities into the right component of $\oplus$:

$$\text{o} \text{plusLiftEERight : } [A : Type] \to (f, g, h : A \to Val) \to (g \oplus h) \to (f \oplus g) \oplus (f \oplus h)$$

$$\text{o} \text{plusLiftEERight } A \ f \ g \ h \ e \ e \ a = \text{cong } (e \ a)$$

### 4.1 Properties of monad algebras

Condition for a function $f$ to be an $M$-algebra homomorphism:

$$\text{algMorSpec : } [A, B : Type] \to (\alpha : M A \to A) \to (\beta : M B \to B) \to (f : A \to B) \to Type$$

$$\text{algMorSpec } A \{B\} \alpha \beta \ f = (\beta \circ \text{map } f) \oplus (f \circ \alpha)$$

Structure maps of $M$-algebras are left inverses of $\text{pure}$:

$$\text{algPureSpec : } [A : Type] \to (\alpha : M A \to A) \to Type$$

$$\text{algPureSpec } A \alpha = \alpha \circ \text{pure} \oplus \text{id}$$

Structure maps of $M$-algebras are themselves $M$-algebra homomorphisms:

$$\text{algJoinSpec : } [A : Type] \to (\alpha : M A \to A) \to Type$$

$$\text{algJoinSpec } A \alpha = \text{algMorSpec } \alpha \alpha \text{ join } \alpha \alpha \text{ -- (} \alpha \circ \text{map } \alpha \text{) } \oplus (\alpha \circ \text{join } \circ \text{map } g)$$

A lemma about computation with $M$-algebras:

$$\text{algLemma : } [A, B, C : Type] \to (\alpha : M C \to C) \to (ee : \text{algJoinSpec } \alpha) \to (f : B \to C) \to (g : A \to M B) \to$$

$$(\alpha \circ \text{map } (\alpha \circ \text{map } f \circ g) \circ \text{join } \circ \text{map } g) \oplus (\alpha \circ \text{map } f \circ \text{join } \circ \text{map } g)$$

$$\text{algLemma } A \{B\} \{C\} \alpha \ e e \ f \ g \ m a =$$

$$\text{=} (\text{cong } \text{mapPresComp } g (\alpha \circ \text{map } f ) \text{ ma} )$$

$$\text{=} (\text{cong } \text{mapPresComp } (\text{map } f ) (\alpha \circ \text{map } g \text{ ma} ) )$$

$$\text{=} (\text{cong } (\text{map } \alpha \circ \text{map } f ) (\text{map } g \text{ ma} ) )$$

$$\text{=} (\text{cong } (\text{sym } (\text{joinNatTrans } f (\text{map } g \text{ ma} ) ) ) )$$

$$\text{=} (\text{cong } \text{map } f \circ \text{join } \circ \text{map } g ) \text{ ma} )$$

### 4.2 Measure specifications

The measure needs to be the structure map of an $M$-algebra on $Val$. This means:

- It is a left inverse to $\text{pure}$:

  $$\text{measPureSpec : algPureSpec meas } \text{ -- meas } \circ \text{pure} \oplus \text{id}$$

- It is an $M$-algebra homomorphism from $\text{join}$ to itself:

  $$\text{measJoinSpec : algJoinSpec meas } \text{ -- meas } \circ \text{join} \oplus \text{meas } \circ \text{map meas}$$
Moreover, for all \(v : Val\), the function \((v \oplus)\) needs to be an \(M\)-algebra homomorphism:

\[
\begin{align*}
\text{measPlusSpec} : (v : Val) &\rightarrow (mv : M Val) \rightarrow (\text{NotEmpty} \; mv) \rightarrow \\
& \quad (\text{meas} \circ \text{map} (v \oplus)) \; \text{mv} = ((v \oplus) \circ \text{meas}) \; \text{mv}
\end{align*}
\]

We can omit the non-emptiness condition but this means we implicitly restrict the class of monads that can be used for \(M\). The condition could then be expressed as

\[
\text{measPlusSpec}^\prime : (v : Val) \rightarrow \text{algMorSpec meas} \; (\oplus \; v)
\]

\section{5 Bellman’s principle of optimality}

Basic requirements for monadic backward induction:

\[
(\subseteq) : Val \rightarrow Val \rightarrow Type
\]

\[
\begin{align*}
\text{lteRefl} & : \{a : Val\} \rightarrow a \subseteq a \\
\text{lteTrans} & : \{a, b, c : Val\} \rightarrow a \subseteq b \implies b \subseteq c \implies a \subseteq c \\
\text{plusMonSpec} & : \{a, b, c, d : Val\} \rightarrow a \subseteq b \implies c \subseteq d \implies (a \oplus c) \subseteq (b \oplus d)
\end{align*}
\]

\[
\text{measMonSpec} : \{A : Type\} \rightarrow (f, g : A \rightarrow Val) \rightarrow ((a : A) \rightarrow (f \; a) \subseteq (g \; a)) \rightarrow \\
\quad (ma : M \; A) \rightarrow \text{meas} \; (\text{map} \; f \; ma) \subseteq \text{meas} \; (\text{map} \; g \; ma)
\]

Optimality of policy sequences:

\[
\text{OptPolicySeq} : \{t, n : \mathbb{N}\} \rightarrow \text{PolicySeq} \; t \; n \rightarrow Type
\]

\[
\text{OptPolicySeq} \; \{t\} \; \{n\} \; ps = (ps' : \text{PolicySeq} \; t \; n) \rightarrow (x : X \; t) \rightarrow \text{val} \; ps' \; x \subseteq \text{val} \; ps \; x
\]

Optimality of extensions of policy sequences:

\[
\text{OptExt} : \{t, n : \mathbb{N}\} \rightarrow \text{PolicySeq} \; (S \; t) \; n \rightarrow \text{Policy} \; t \rightarrow Type
\]

\[
\text{OptExt} \; \{t\} \; ps \; p = (p' : \text{Policy} \; t) \rightarrow (x : X \; t) \rightarrow \text{val} \; (p' :: ps) \; x \subseteq \text{val} \; (p :: ps) \; x
\]

Bellman’s principle of optimality:

\[
\text{Bellman} : \{t, n : \mathbb{N}\} \rightarrow (ps : \text{PolicySeq} \; (S \; t) \; n) \rightarrow \text{OptPolicySeq} \; ps \rightarrow \\
\quad (p : \text{Policy} \; t) \rightarrow \text{OptExt} \; ps \; p \rightarrow \text{OptPolicySeq} \; (p :: ps)
\]

\[
\text{Bellman} \; \{t\} \; ps \; ops \; p \; \text{oop} \; (p' :: ps') \; x =
\]

\[
\begin{align*}
\text{let } y' & = p' \; x & \in \\
\text{let } mx' & = \text{next} \; t \; x \; y' & \in \\
\text{let } f' & = \text{reward} \; t \; x \; y' \oplus \text{val} \; ps' & \in \\
\text{let } f & = \text{reward} \; t \; x \; y' \oplus \text{val} \; ps & \in \\
\text{let } s_0 & = \lambda x \Rightarrow \text{plusMonSpec} \; \text{lteRefl} \; (\text{ops} \; ps' \; x') & \in \\
\text{let } s_1 & = \text{measMonSpec} \; f' \; f \; s_0 \; mx' & \in \quad \text{val} \; (p' :: ps') \; x \subseteq \text{val} \; (p' :: ps) \; x \\
\text{let } s_2 & = \text{ooe} \; p' \; x & \in \quad \text{val} \; (p' :: ps) \; x \subseteq \text{val} \; (p :: ps) \; x \\
\text{lteRefl} \; s_1 \; s_2
\end{align*}
\]

\section{6 Verification with respect to val}

The empty policy sequence is optimal:

\[
\begin{align*}
\text{nilOptPolicySeq} : & \text{OptPolicySeq} \; \text{Nil} \\
\text{nilOptPolicySeq} \; \text{Nil} \; x = & \; \text{lteRefl}
\end{align*}
\]

Now, provided that we can implement
optExt : \{t, n : \mathbb{N}\} \rightarrow \text{PolicySeq}(S t) n \rightarrow \text{Policy} t
optExtSpec : \{t, n : \mathbb{N}\} \rightarrow (ps : \text{PolicySeq}(S t) n) \rightarrow \text{OptExt} ps (optExt ps)

then

\begin{align*}
bi : (t : \mathbb{N}) \rightarrow (n : \mathbb{N}) \rightarrow \text{PolicySeq} t n \\
bi t Z &= \text{Nil} \\
bi t (S n) &= \text{let } ps = bi (S t) n \text{ in } \text{optExt} ps :: ps
\end{align*}

is correct with respect to \text{val}:

\begin{align*}
\text{biOptVal} : (t : \mathbb{N}) \rightarrow (n : \mathbb{N}) \rightarrow \text{OptPolicySeq}(bi t n) \\
\text{biOptVal} t Z &= \text{nilOptPolicySeq} \\
\text{biOptVal} t (S n) &= \\
&= \text{let } ps = bi (S t) n \text{ in } \\
&\quad \text{let } ops = \text{biOptVal} (S t) n \text{ in } \\
&\quad \text{let } p = \text{optExt} ps \text{ in } \\
&\quad \text{let } oep = \text{optExtSpec} ps \text{ in } \\
&\quad \text{Bellman } ps \text{ ops } p \text{ oep}
\end{align*}

7 Optimal extension

The generic implementation of backward induction \text{bi} naturally raises the question under which conditions one can implement \text{optExt} such that \text{optExtSpec} holds.

To this end, consider the function

\begin{align*}
cval : \{t, n : \mathbb{N}\} \rightarrow \text{PolicySeq}(S t) n \rightarrow (x : X t) \rightarrow Y t x \rightarrow \text{Val} \\
cval \{t\} ps x y &= \text{let } mx' = \text{next } t x y \text{ in } \\
&\quad \text{meas}(\text{map}(\text{reward } t x y \bigoplus \text{val} \ ps) mx')
\end{align*}

By definition of \text{val} and \text{cval}, one has

\begin{align*}
\text{val}(p :: ps) x &= \\
&= \text{meas}(\text{map}(\text{reward } t x (p. x) \bigoplus \text{val} \ ps) (\text{next } t x (p. x))) \\
&= cval ps x (p. x)
\end{align*}

This suggests that, if we can maximise \text{cval}, i.e. implement

\begin{align*}
cvalmax : \{t, n : \mathbb{N}\} \rightarrow \text{PolicySeq}(S t) n \rightarrow (x : X t) \rightarrow \text{Val} \\
cvalargmaxmax : \{t, n : \mathbb{N}\} \rightarrow \text{PolicySeq}(S t) n \rightarrow (x : X t) \rightarrow Y t x
\end{align*}

that fulfill

\begin{align*}
cvalmaxSpec : \{t, n : \mathbb{N}\} \rightarrow (ps : \text{PolicySeq}(S t) n) \rightarrow (x : X t) \rightarrow \\
&\quad (y : Y t x) \rightarrow \text{cvalmax} ps x y \sqsubseteq \text{cvalmaxSpec} ps x \\
cvalargmaxSpec : \{t, n : \mathbb{N}\} \rightarrow (ps : \text{PolicySeq}(S t) n) \rightarrow (x : X t) \rightarrow \\
&\quad \text{cvalmaxSpec} ps x = \text{cval max} ps x (\text{cvalargmaxSpec} ps x)
\end{align*}

then we can implement optimal extensions of arbitrary policy sequences. As it turns out, this intuition is correct. With

\begin{align*}
onoptExt = cvalargmax
\end{align*}
one has

\[
\text{optExtSpec } \{ t \} \{ n \} \text{ ps } p' \text{ x } = \\
\text{let } p \text{ = optExt } \text{ ps } \text{ in} \\
\text{let } y \text{ = } p \text{ x } \text{ in} \\
\text{let } y' \text{ = } p' \text{ x } \text{ in} \\
\text{let } s1 = \text{cvalmaxSpec } \text{ ps } x \text{ y'} \text{ in} \\
\text{let } s2 = \text{replace } \{ P = \lambda z \Rightarrow (\text{cval } \text{ ps } x \text{ y'} \subseteq z) \} (\text{cvalargmaxSpec } \text{ ps } x) \text{ s1 } \text{ in} \\
\text{s2}
\]

The observation that functions \text{cvalmax} and \text{cvalargmax} that fulfil \text{cvalmaxSpec} and \text{cvalargmaxSpec} are sufficient to implement an optimal extension \text{optExt} that fulfils \text{optExtSpec} naturally raises the question of what are necessary and sufficient conditions for \text{cvalmax} and \text{cvalargmax}. Answering this question necessarily requires discussing properties of \text{cval} and goes well beyond the scope of formulating a theory of SDPs. Here, we limit ourselves to remark that if \text{Ytx} is finite and non-empty one can implement the functions \text{cvalmax} and \text{cvalargmax} by linear search. A generic implementation of \text{cvalmax} and \text{cvalargmax} can be found under Brede & Botta (2021).

For the original BJI-theory, tabulated backward induction and several example applications can be found in the \text{SequentialDecisionProblems} folder of Botta (2016–2021).