Derived Automata and an Application to Markov Reward Chains

MOVES Seminar

Tobias Winkler

25.06.2020

Software Modeling and Verification Chair
RWTH AACHEN UNIVERSITY

Outline

1. Derivatives of weighted automata

2. Markov chains with rewards

3. Expected values of ratios

Semirings

Definition

A semiring $(A, +, \cdot, 0, 1)$ is a ring where existence of negative elements is optional.

Examples:

- Every ring
- $\mathbb{N}$ and $\mathbb{R}_{\geq 0}$
- $\mathbb{N} \cup \{\infty\}$ and $\mathbb{R}_{\geq 0} \cup \{\infty\}$ (with $\infty \cdot 0 = 0$)
- $(\mathbb{N} \cup \{\infty\}, \min, +, \infty, 0)$ the *tropical* semiring
- $(2^{\Sigma^*}, \cup, \cdot, \emptyset, \{\epsilon\})$ the semiring of *formal languages*

Let A be a semiring.

Definition

An A-weighted automaton $\mathfrak{A}$ consists of

- a finite index set S (states)
- a transition matrix $T \in A^{S \times S}$
- an initial vector $I \in A^S$
- a final vector $F \in A^S$

The behaviour of automaton $\mathfrak{A}$ is defined* as

$$|\mathfrak{A}| = IT^0F + IT^1F + \ldots = IT^*F \in A$$

*under a few additional conditions

You all know weighted automata!

A Markov chain with reach property $\Diamond B$ is an $\mathbb{R}_{\geq 0}$-weighted automaton:

- T is the transition probability matrix*
- I is the initial distribution
- F is the characteristic vector of set B

$$|\mathfrak{A}| = Pr(\Diamond B)$$

*outgoing transitions of states in B removed

Derivatives in semirings

Definition

A mapping $\partial\colon A \to A$ in semiring A is called derivation if

- $\partial(x + y) = \partial x + \partial y$
- $\partial(xy) = \partial x \cdot y + x \cdot \partial y$

Examples:

- Polynomials over a semiring with their usual differentiation:

$$\partial(3x^2 + 5x + 2) = 6x + 5$$

- Formal power series (“infinite polynomials”)
- Matrix semirings with pointwise extension of ∂

The “derived” automaton $\partial\mathfrak{A}$

Let A be a semiring with derivation ∂.

Definition

Let $\mathfrak{A} = (I, T, F)$ be an A-automaton. Its derivation $\partial\mathfrak{A}$ has

- Transition matrix $\begin{pmatrix} T & 0 \\ \partial T & T \end{pmatrix}$
- Initial vector $\begin{pmatrix} 0 & I \end{pmatrix}$
- Final vector $\begin{pmatrix} F & 0 \end{pmatrix}$

Theorem

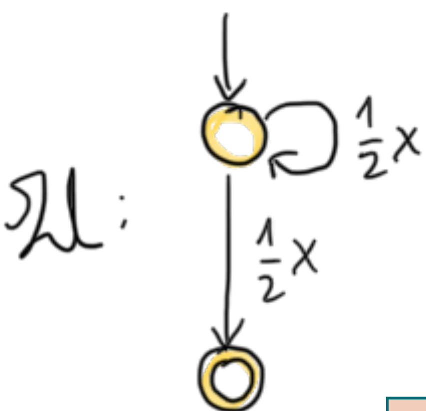
$$|\,\partial\mathfrak{A}\,| = \partial\,|\,\mathfrak{A}\,|$$

Example

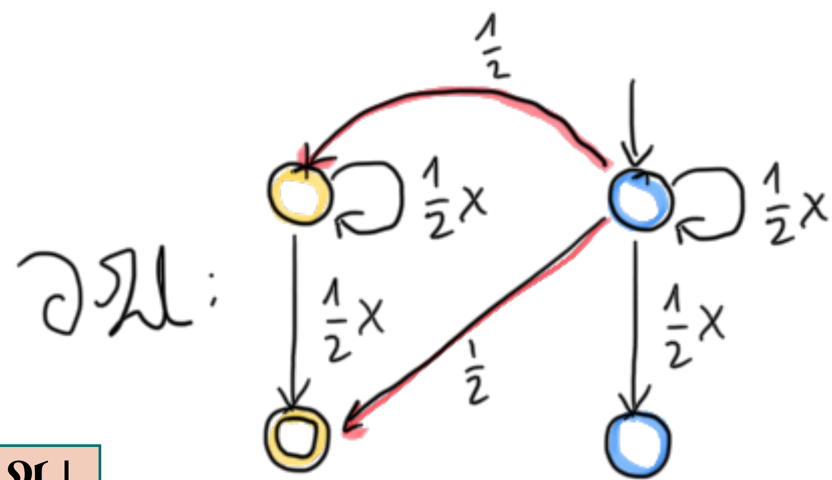
Definition *(from previous slide)*

Let $\mathfrak{A} = (I, T, F)$ be an A-automaton. Its derivation $\partial\mathfrak{A}$ has

- Transition matrix $\begin{pmatrix} T & 0 \\ \partial T & T \end{pmatrix}$
- Initial vector $(0 \quad I)$
- Final vector $(F \quad 0)$



$$|\,\partial\mathfrak{A}\,| = \partial\,|\,\mathfrak{A}\,|$$



Homomorphism applied to automaton

Let A, B be semirings, $\phi : A \to B$ a semiring-homomorphism

Definition

Let $\mathfrak{A} = (I, T, F)$ be an A-automaton. Define $\phi\mathfrak{A}$ as the B-automaten

- Transition matrix ϕT
- Initial vector ϕI
- Final vector ϕF

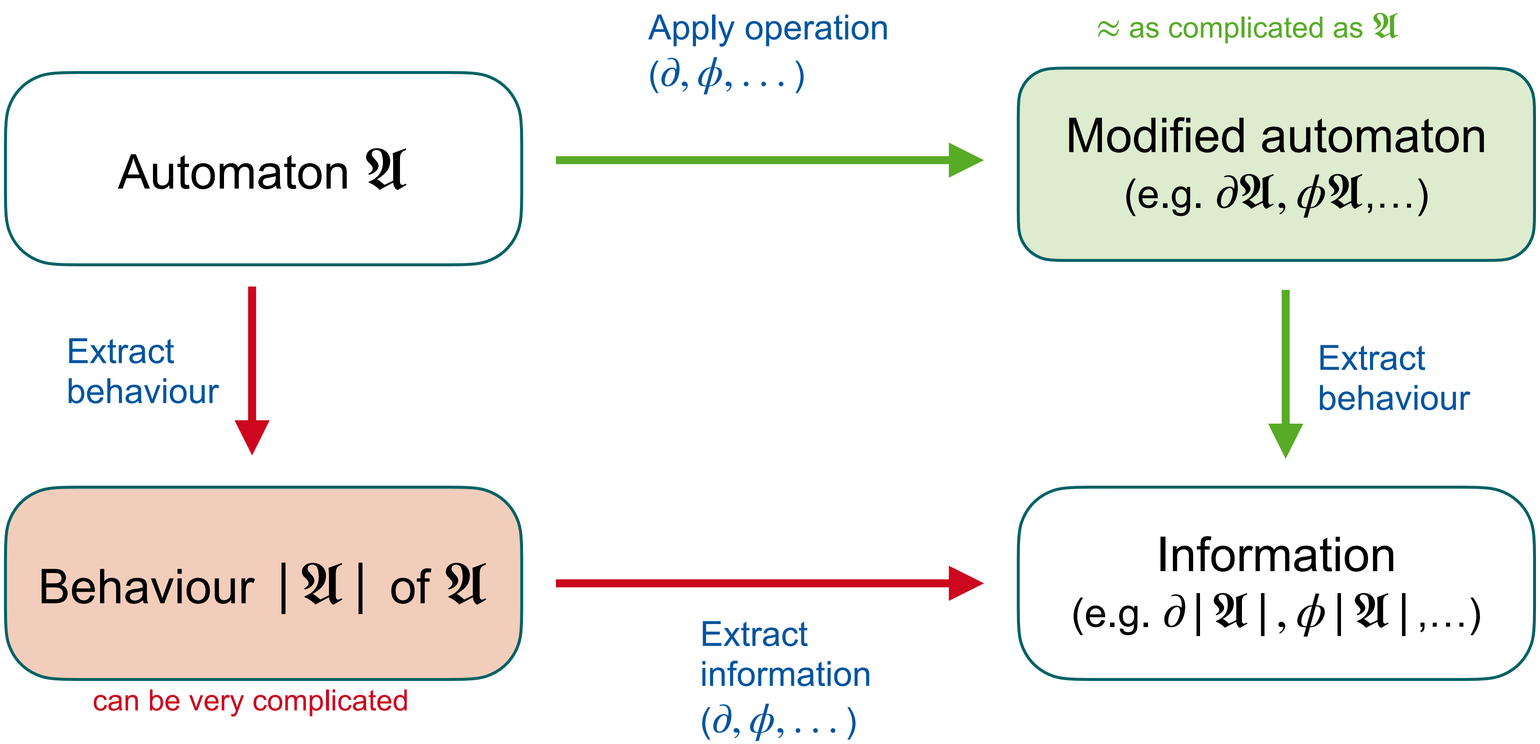
(all these applications are pointwise)

Proposition

$$|\phi\mathfrak{A}| = \phi|\mathfrak{A}|$$

The general principle

> *Fact*
>
> Applying operations like ∂, ϕ (and others) to the behaviour $|\mathfrak{A}|$ often yields useful information.

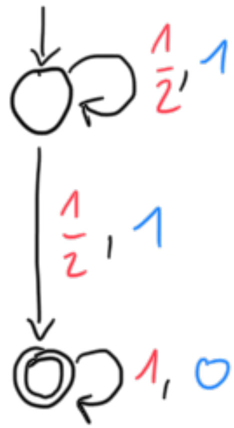


Outline

1. Derivatives of weighted automata
2. Markov chains with rewards
3. Expected values of ratios

Markov chains with rewards

- Transitions carry a probability *and* a reward $r : S \times S \to \mathbb{Z}_{\geq 0}$
- Now: Expected reward until reaching a target $B \subseteq S$



- Is this a *weighted automaton*? If yes, what is the underlying *semiring*?

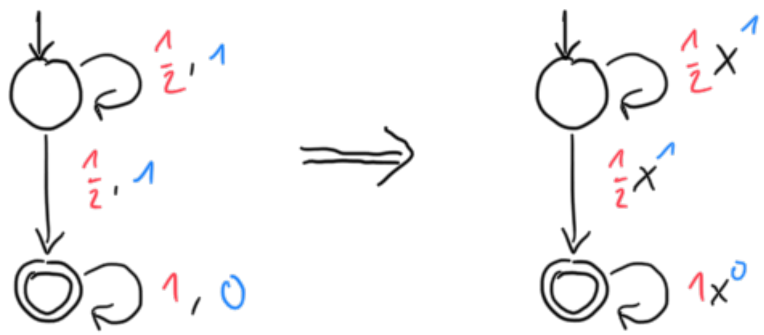
Encoding probabilities and rewards

Transitions carry two kinds of quantitative information:

- probabilities are *multiplied* along a path
- rewards are *added* along a path

This can be encoded as *multiplication of polynomials*:

$$p_1 x^{r_1} \cdot p_2 x^{r_2} = p_1 \cdot p_2 \, x^{r_1 + r_2}$$

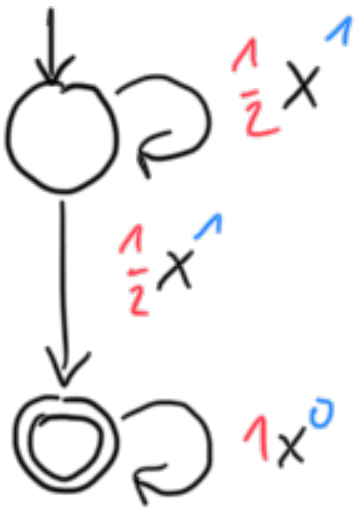


What is the behaviour of the resulting weighted automaton?

Software Modeling and Verification Chair

RWTH AACHEN UNIVERSITY

The Probability Generating Function



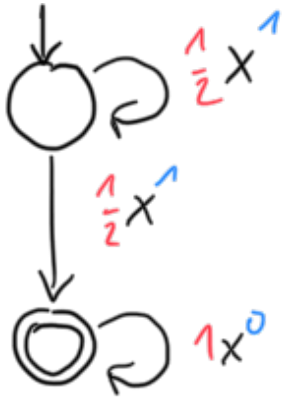
$$|\mathfrak{A}| = \sum_{k\geq 0} IT^k F$$
$$= 0 + \sum_{k\geq 1} IT^k F$$
$$= 0 + \frac{1}{2}x + \sum_{k\geq 2} IT^k F$$
$$= 0 + \frac{1}{2}x + \frac{1}{4}x^2 + \sum_{k\geq 3} IT^k F$$
$$\ldots$$
$$= 0 + \frac{1}{2}x + \frac{1}{4}x^2 + \frac{1}{8}x^3 + \ldots$$

This *infinite power series* is the probability generating function (PGF)
(of the RV modelling total reward until reaching the target)

Extracting information from a PGF

- PGF:

$$|\mathfrak{A}| = \frac{1}{2}x + \frac{1}{4}x^2 + \frac{1}{8}x^3 + \ldots$$



- Expected value:

$$\mathbb{E} = \sum_{k \geq 0} k \cdot \mathbb{P}(k) = 1 \cdot \frac{1}{2} + 2 \cdot \frac{1}{4} + 3 \cdot \frac{1}{8} + \ldots = \phi \partial |\mathfrak{A}|$$

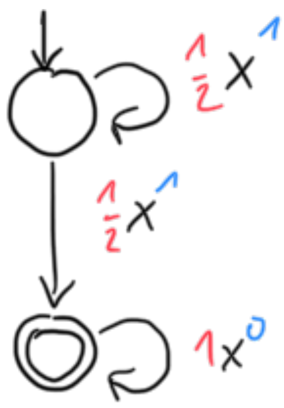
where ϕ is the homomorphism that substitutes $x = 1$.

An automaton for the expected reward

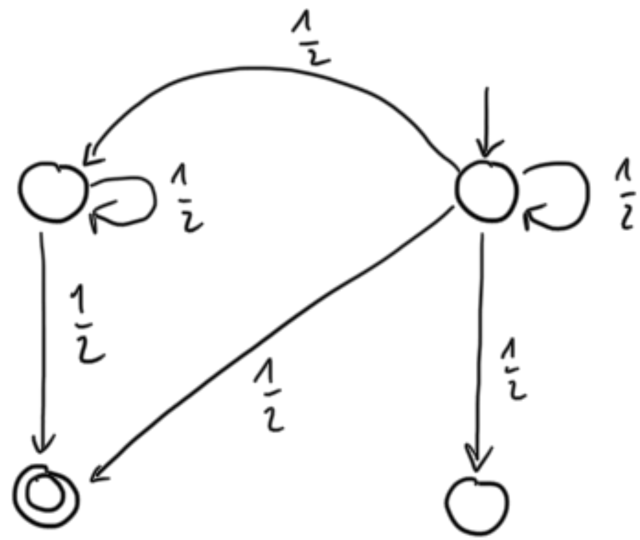
Expected value: $\mathbb{E} = \phi\partial\,|\,\mathfrak{A}\,|$

$$\phi\partial\,|\,\mathfrak{A}\,| = |\,\phi\partial\mathfrak{A}\,|$$

$\mathfrak{A}$:



$\phi\partial\mathfrak{A}$:



Fixpoint iteration for expected rewards

In general $|\phi\partial\mathfrak{A}|$ is the least fixpoint of

$$\mathbb{E}_s = \begin{cases} 0 & \text{if } s \in B \\ \sum_{s'} p_{s,s'}\left(r_{s,s'} \cdot \mathbb{P}_{s'} + \mathbb{E}_{s'}\right) & \text{else.} \end{cases}$$

We automatically get fixpoint operators for higher moments too, e.g.

$$\mathbb{E}_s(R^2) = \begin{cases} 0 & \text{if } s \in B \\ \sum_{s'} p_{s,s'}\left(r_{s,s'}^2 + 2r_{s,s'}\mathbb{E}_{s'}(R) + \mathbb{E}_{s'}(R^2)\right) & \text{else.} \end{cases}$$

(if all states reach B almost-surely)

Some observations

Conjectures

- *There is a linear fixpoint operator for $\mathbb{E}(f(R))$ for every polynomial f.*
- *This can be generalised to multiple reward functions.*
- $\mathbb{E}(f(R_1, \ldots, R_n))$ *is a rational number* *(if transitions prob's/coeff's are rational)*.

Outline

1. Derivatives of weighted automata
2. Markov chains with rewards
3. Expected values of ratios

A probabilistic program

```
x = 0;
flag = true;
while(flag) {
        x++;
        { skip; } [1/2] { flag=false; }
}
{ y = 1; } [1/x] { y = 0; }
```

What is the probability that y = 1 after termination?

$$\mathbb{E}\left(\frac{1}{x}\right) = ln(2) \approx 0.69\ldots$$

> *This quantity is not rational (not even algebraic), so expected values of rational functions are fundamentally different from polynomials.*

Model checking expected ratios

Can we recover $\mathbb{E}\left(\frac{1}{R}\right)$ from the PGF $\mid \mathfrak{A} \mid$?

$$\mathbb{E}\left(\frac{1}{R}\right) = \sum_{k \geq 0} \frac{1}{k} \cdot \mathbb{P}(k) = \int_0^1 \frac{1}{x} \cdot \mid \mathfrak{A} \mid dx$$

Assume $\mathbb{P}(R = 0) = 0$ for now.

Integrating the generating function

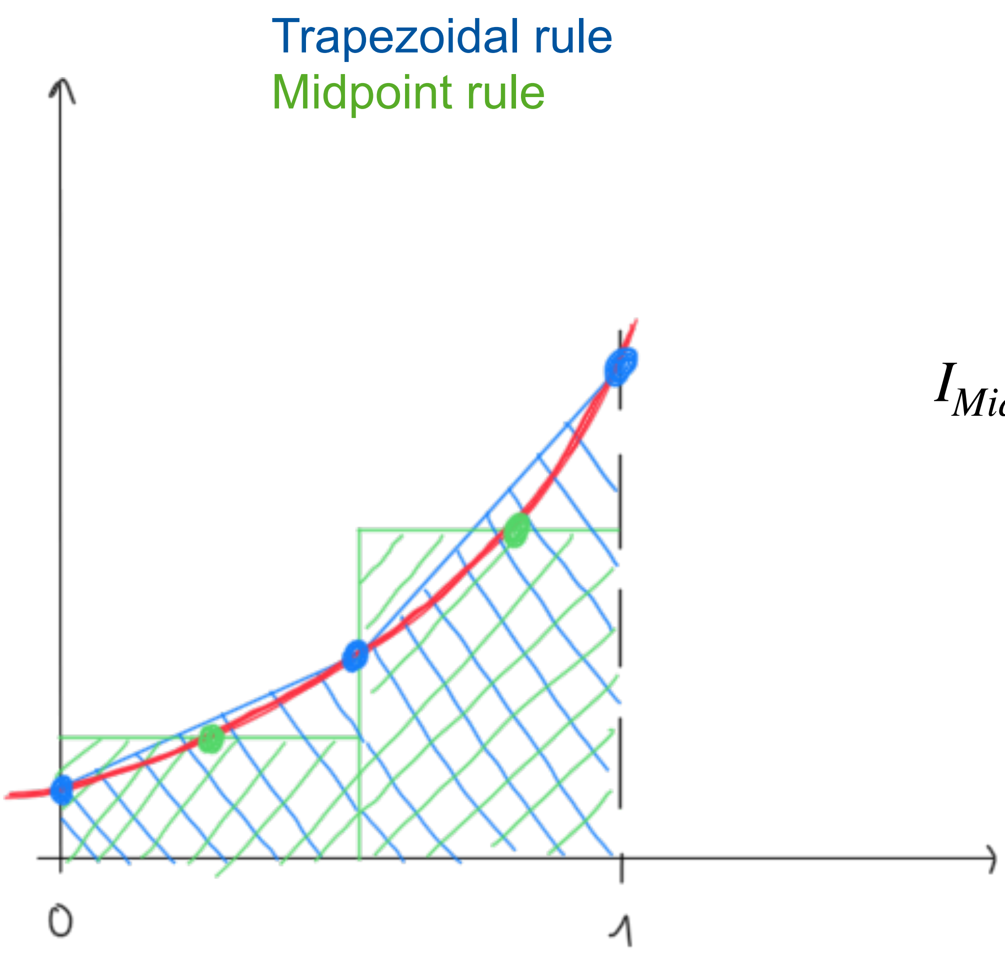
$$\mathbb{E}\left(\frac{1}{R}\right) = \int_0^1 \frac{1}{x} \,|\, \mathfrak{A} \,|\, dx$$

- Want compute sound upper/lower bounds on this
- Use standard numeric integration techniques
- Evaluate the PGF using "value iteration" from above/below

Lemma

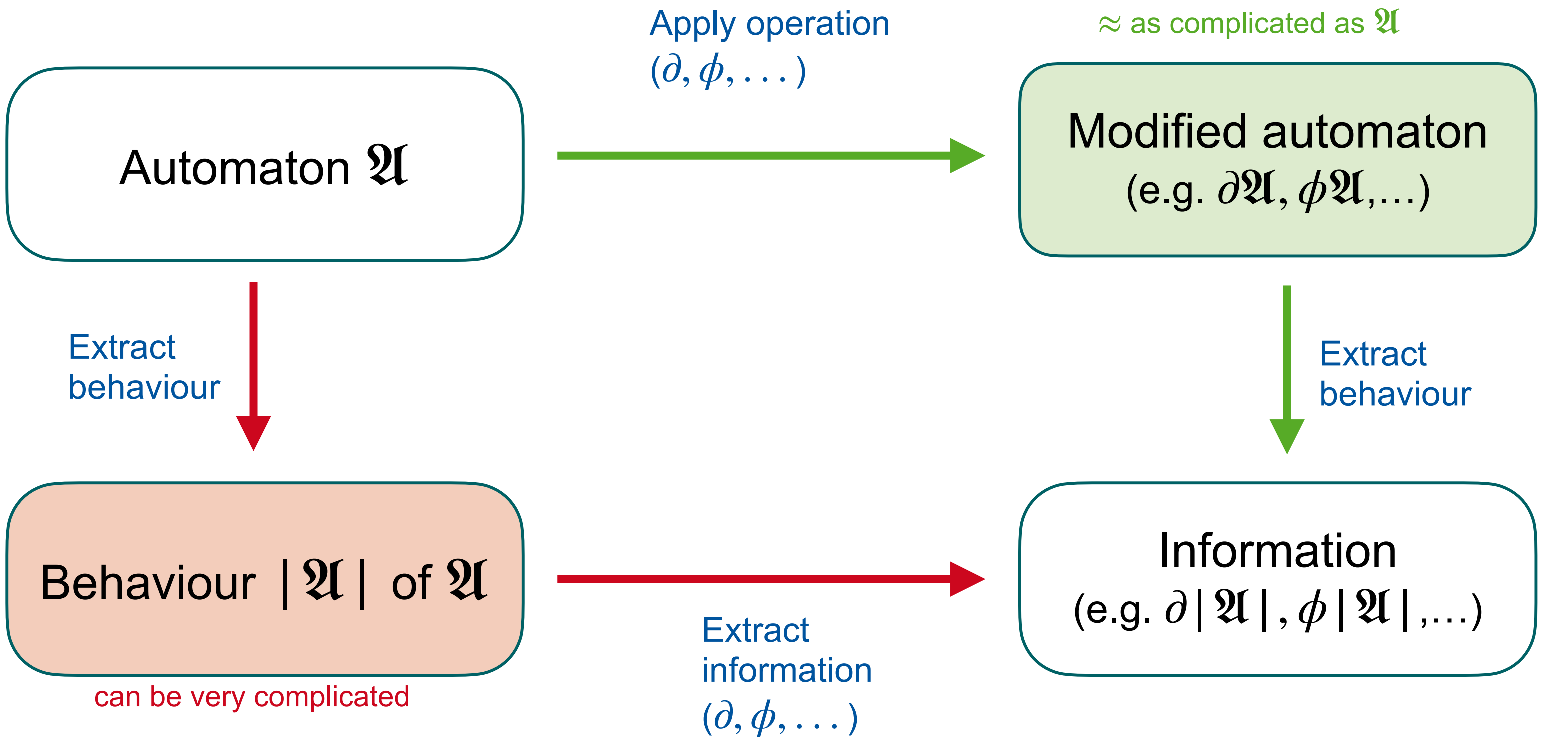
The function $\frac{1}{x} \,|\, \mathfrak{A} \,|$ *is convex on [0,1].*

Numeric integration of a convex function



$$I_{Midpoint} \leq I_{exact} \leq I_{Trapezoidal}$$

Summary



We have applied this principle to

- expected rewards and polynomial combinations thereof
- expected values of reward ratios

Thank you!