A Probabilistic Temporal Epistemic Logic

Zoran Ognjanović, Angelina Ilić Stepić, Aleksandar Perović

LAP 2021, Dubrovnik

Outline

Logical Framework for Proving the Correctness of the Chord Protocol

Bojan Marinković, Paola Glavan and Zoran Ognjanović

- Blockchain is a multiagent dynamically distributed system without third authority, which synchronizes and maintains copies of a distributed append-only ledger which records transactions (transfers of some units of crypto-currency, smart contracts, etc.)

- Protcol defines hard problem, a cryptographic puzzle, and each agent tries to solve this problem
- If an agent solves the problem first, his solution is accepted and all other agents add that solution to their own ledger
- It may happen, with small probabiliy that (two) agents have different solutions
- Fork is situation when agents simultaneously receive several solutions. This happens with low probability

- For this purpose we develop a complex logic that has temporal epistemic and probabilistic aspects

Syntax and semantics

- $\mathbb{N}$-the set of nonnegative integers,
- $[0,1]_{\mathbb{Q}}$ the set of all rational numbers from the unit interval
- $\mathbb{P}(A)$ the powerset set of a set A
- $\mathbb{A}$ - the set of agents $\{a_1, \ldots, a_m\}$, where m is a positive integer.

Syntax and semantics

The formal language of **PTEL** consists of a nonempty at most countable set of propositional letters denoted **Var** and the following operators:

- classical: $\neg$, $\wedge$,
- temporal: $\bigcirc$, $\mathtt{U}$, $\bullet$, $\mathtt{S}$,
- epistemic: $\mathtt{K}_a$, $\mathtt{C}$, where $a \in \mathbb{A}$,
- probabilistic: $\mathtt{P}_{\geqslant s}$, $\mathtt{P}_{a,\geqslant s}$, where $a \in \mathbb{A}$, $s \in [0,1]_{\mathbb{Q}}$.

Syntax and semantics

- $\mathbf{Var} \supseteq \mathbf{A} = \{A_a | a \in \mathbb{A}\}$
- A_a : "agent a is active"
- **For** denotes the set of formulas defined in the usual way.
- the lowercase Latin letters p and q, possibly with indices, denote propositional variables, and
- the lowercase Greek letters α, β, γ, ... denote formulas.

$$\mathrm{E}\alpha =_{def} \bigwedge_{a \in \mathbf{A}} \mathrm{K}_a \alpha$$

.

Syntax and semantics

- $\mathtt{F}\alpha =_{def} (\alpha \to \alpha)\mathtt{U}\alpha$,
- $\mathtt{P}\alpha =_{def} (\alpha \to \alpha)\mathtt{S}\alpha$,
- $\mathtt{G}\alpha =_{def} \neg\mathtt{F}\neg\alpha$
- $\mathtt{H}\alpha =_{def} \neg\mathtt{P}\neg\alpha$

Syntax and semantics

Definition

A model $\mathcal{M}$ is any tuple $\langle \mathbf{R}, \mathcal{A}, \mathcal{K}, \mathcal{P} \rangle$ such that

- $\mathbf{R}$ is a non-empty set of runs, where:
  - Every *run* r is a function from $\mathbb{N}$ to $\mathbb{P}(\mathbf{Var})$.
  - The pair (r, n), where $r \in \mathbf{R}$ and $n \in \mathbb{N}$, is called a *possible world*; the set of all possible worlds in $\mathcal{M}$ is denoted by $\mathbf{W}$.
- $\mathcal{A}$ is a function from the set of possible world $\mathbf{W}$ to $\mathbb{P}(\mathbb{A})$, where:
  - $\mathcal{A}((r, n))$ denotes the set of *active agents* associated to the possible world (r, n), and
  - $a \in \mathcal{A}((r, n))$ iff $A_a \in r(n)$.

Syntax and semantics

Definition

- $\mathcal{K} = \{\mathcal{K}_a : a \in \mathbb{A}\}$ is the set of symmetric and transitive binary *accessibility relations* on $\mathbf{W}$, such that:
  - $a \notin \mathcal{A}((r,n))$ iff $(r,n)\mathcal{K}_a(r',n')$ is false for all (r',n').
  - $\mathcal{K}_a(r,n)$ denotes the set of all possible worlds *accessible*, according to the agent a, from (r,n).
  - If $a \in \mathcal{A}((r,n))$, then $(r,n)\mathcal{K}_a(r,n)$.

Syntax and semantics

Definition

- $\mathcal{P}$ is a functions defined on $\mathbf{W}$, where
  - $\mathcal{P}((r,n)) = \langle H^{(r,n)}, \mu^{(r,n)}, \{\mathcal{P}_a : a \in \mathbb{A}\}\rangle$,
  - $H^{(r,n)}$ is an algebra of subsets of $\mathbf{R}$,
  - $\mu^{(r,n)} : H^{(r,n)} \to [0,1]$ is a finitely-additive probability measure on $H^{(r,n)}$,
  - $\{\mathcal{P}_a : a \in \mathbb{A}\}$ is the set of functions defined on $\mathbf{W}$, where $\mathcal{P}_a((r,n)) = \langle \mathbf{W}_a^{(r,n)}, H_a^{(r,n)}, \mu_a^{(r,n)}\rangle$ is a probability space such that:
    - $\mathbf{W}_a^{(r,n)}$ is a non-empty subset of $\mathbf{W}$,
    - $H_a^{(r,n)}$ is an algebra of subsets of $\mathbf{W}_a^{(r,n)}$, and
    - $\mu_a^{(r,n)} : H_a^{(r,n)} \to [0,1]$ is a finitely-additive probability measure. ■

$$\mu_{\star,a}^{(r,n)}(\mathbf{X}) = \sup\{\mu_a^{(r,n)}(\mathbf{Y}) \,:\, \mathbf{Y} \subset \mathbf{X}, \mathbf{Y} \in H_a^{(r,n)}\}$$

Syntax and semantics

Definition

Let $\mathcal{M} = \langle \mathbf{R}, \mathcal{A}, \mathcal{K}, \mathcal{P} \rangle$ be a model. The satisfiability relation $\models$ fulfils:

1. if $p \in \mathbf{Var}$, $(r, n) \models p$ iff $p \in r(n)$,
2. $(r, n) \models \alpha \wedge \beta$ iff $(r, n) \models \alpha$ and $(r, n) \models \beta$,
3. $(r, n) \models \neg\beta$ iff not $(r, n) \models \beta$ (i.e., $(r, n) \not\models \beta$),
4. $(r, n) \models \bigcirc\beta$ iff $(r, n+1) \models \beta$,
5. $(r, n) \models \alpha \mathrm{U} \beta$ iff there is an integer $j \geqslant n$ such that $(r, j) \models \beta$, and for every integer k, such that $n \leqslant k < j$, $(r, k) \models \alpha$,
6. $(r, n) \models \bullet\beta$ iff $n = 0$, or $n \geqslant 1$ and $(r, n-1) \models \beta$,
7. $(r, n) \models \alpha \mathrm{S} \beta$ iff there is an integer $j \in [0, n]$ such that $(r, j) \models \beta$, and for every integer k, such that $j < k \leqslant n$, $(r, k) \models \alpha$

Syntax and semantics

Definition

8. $(r, n) \models \mathtt{K}_a \beta$ iff $(r', n') \models \beta$ for all $(r', n') \in \mathcal{K}_a(r, n)$,
9. $(r, n) \models \mathtt{C}\beta$ iff for every integer $k \geqslant 0$, $(r, n) \models \mathtt{E}^k \beta$,
10. $(r, n) \models \mathtt{P}_{\geqslant s} \beta$ iff $\mu_\star^{(r,n)}(\{r \in \mathbf{R} : (r, 0) \models \beta\}) \geqslant s$.
11. $(r, n) \models \mathtt{P}_{a, \geqslant s} \beta$ iff $\mu_{\star,a}^{(r,n)}(\{(r', n') \in \mathbf{W}_a^{(r,n)} : (r', n') \models \beta\}) \geqslant s$. ■

Non-compactness

- $\{\bigcirc^k \alpha \ : \ k \in \mathbb{N}\} \cup \{\neg \mathtt{G}\alpha\}$,
- $\{\mathtt{E}^k \alpha \ : \ k \in \mathbb{N}\} \cup \{\neg \mathtt{C}\alpha\}$,
- $\{\mathcal{P}_{\leqslant 1/k}\alpha \ : \ k \in \mathbb{N}\} \cup \{\neg \mathcal{P}_{=0}\alpha\}$, etc.

Strongly complete axiomatization, system Ax_{PTEL}

I Propositional axioms and rules

Prop. All instances of classical propositional tautologies

MP. $$\frac{\alpha, \alpha \rightarrow \beta}{\beta}$$

Strongly complete axiomatization, system Ax_{PTEL}

II Axioms and rules for reasoning about time

A$\bigcirc\neg$.	$\neg\bigcirc\alpha \leftrightarrow \bigcirc\neg\alpha$
A$\bigcirc\rightarrow$.	$\bigcirc(\alpha \rightarrow \beta) \rightarrow (\bigcirc\alpha \rightarrow \bigcirc\beta)$
AU$\bigcirc$.	$\alpha \mathrm{U} \beta \leftrightarrow \beta \vee (\alpha \wedge \bigcirc(\alpha \mathrm{U} \beta))$
AUF.	$\alpha \mathrm{U} \beta \rightarrow \mathrm{F}\beta$
A$\bullet\neg$.	$\neg\bullet\neg\alpha \rightarrow \bullet\alpha$
A$\bullet\rightarrow$.	$\bullet(\alpha \rightarrow \beta) \rightarrow (\bullet\alpha \rightarrow \bullet\beta)$
A$\bullet\wedge$.	$(\bullet\alpha \wedge \bullet\beta) \rightarrow \bullet(\alpha \wedge \beta)$
A$\bigcirc\bullet$.	$\bigcirc\bullet\alpha \leftrightarrow \alpha$
A$\bigcirc\bullet$C$_1$.	$\bigcirc\bullet\alpha \rightarrow \bullet\bigcirc\alpha$
A$\bigcirc\bullet$C$_2$.	$\neg\bullet(\gamma \wedge \neg\gamma) \rightarrow (\bigcirc\bullet\alpha \leftrightarrow \bullet\bigcirc\alpha)$
AS$\bullet$.	$\alpha \mathrm{S} \beta \leftrightarrow [\beta \vee (\neg\bullet(\alpha \wedge \neg\alpha) \wedge [\alpha \wedge \bullet(\alpha \mathrm{S} \beta)])]$
AP$\bullet$.	$\mathrm{P}\bullet\beta$

Strongly complete axiomatization, system Ax_{PTEL}

II Axioms and rules for reasoning about time

- R◯N. $\dfrac{\alpha}{\bigcirc\alpha}$
- R●N. $\dfrac{\alpha}{\bullet\alpha}$
- RU. $\dfrac{\{\Phi_{k,\mathbf{B},\mathbf{X}}(\neg((\bigwedge_{l=0}^{i-1}\bigcirc^{l}\alpha)\wedge\bigcirc^{i}\beta)) \,:\, i\in\mathbb{N}\}}{\Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\alpha \mathrm{U} \beta))}$
- RS. $\dfrac{\{\Phi_{k,\mathbf{B},\mathbf{X}}(\neg((\bigwedge_{l=0}^{i-1}\bullet^{l}\alpha)\wedge(\bigwedge_{l=0}^{i}\neg\bullet^{l}(\alpha\wedge\neg\alpha))\wedge\bullet^{i}\beta)) \,:\, i\in\mathbb{N}\}}{\Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\alpha \mathrm{S} \beta))}$

Strongly complete axiomatization, system Ax_{PTEL}

III Axioms and rules for reasoning about knowledge

AK→.	$\mathrm{K}_a(\alpha \to \beta) \to (\mathrm{K}_a\alpha \to \mathrm{K}_a\beta)$
AKR.	$A_a \to (\mathrm{K}_a\alpha \to \alpha)$
AKA.	$A_a \to \mathrm{K}_a A_a$
AKDE.	$\neg A_a \to \mathrm{K}_a(\alpha \wedge \neg\alpha)$
AKS.	$\mathrm{K}_a\neg\alpha \to \mathrm{K}_a\neg\mathrm{K}_a\alpha$
AKT.	$\mathrm{K}_a\alpha \to \mathrm{K}_a\mathrm{K}_a\alpha$
ACE.	$\mathrm{C}\alpha \to \mathrm{E}^m\alpha,\ m \in \mathbb{N}$
RK$_a$N.	$\dfrac{\alpha}{\mathrm{K}_a\alpha}$
RC.	$\dfrac{\{\Phi_{k,\mathbf{B},\mathbf{X}}(\mathrm{E}^i\alpha)\ :\ i \in \mathbb{N}\}}{\Phi_{k,\mathbf{B},\mathbf{X}}(\mathrm{C}\alpha)}$

Strongly complete axiomatization, system Ax_{PTEL}

IV Axioms and rules for reasoning about probability on runs

AGP1. $P_{\geqslant 0}\alpha$

AGP2. $P_{\leqslant r}\alpha \rightarrow P_{<t}\alpha$, $t > r$

AGP3. $P_{<t}\alpha \rightarrow P_{\leqslant t}\alpha$

AGP4. $(P_{\geqslant r}\alpha \wedge P_{\geqslant t}\beta \wedge P_{\geqslant 1}\neg(\alpha \wedge \beta)) \rightarrow P_{\geqslant \min(1,r+t)}(\alpha \vee \beta)$

AGP5. $(P_{\leqslant r}\alpha \wedge P_{<t}\alpha) \rightarrow P_{<r+t}(\alpha \vee \beta)$, $r + t \leqslant 1$

AGP●. $P_{\geqslant 1}\bullet(\alpha \wedge \neg\alpha)$

RGPN. $\dfrac{\alpha}{P_{\geqslant 1}\alpha}$

RGA. $\dfrac{\{\Phi_{k,\mathbf{B},\mathbf{X}}(P_{\geqslant r-\frac{1}{i}}\alpha) \,:\, i \geqslant \frac{1}{r}\}}{\Phi_{k,\mathbf{B},\mathbf{X}}(P_{\geqslant r}\alpha)}$, $r \in (0,1]_{\mathbb{Q}}$

Strongly complete axiomatization, system Ax_{PTEL}

V Axioms and rules for reasoning about probability on possible worlds

AP1. $P_{a,\geqslant 0}\alpha$

AP2. $P_{a,\leqslant r}\alpha \rightarrow P_{a,<t}\alpha,\ t > r$

AP3. $P_{a,<t}\alpha \rightarrow P_{a,\leqslant t}\alpha$

AP4. $(P_{a,\geqslant r}\alpha \wedge P_{a,\geqslant t}\beta \wedge P_{a,\geqslant 1}\neg(\alpha \wedge \beta)) \rightarrow P_{a,\geqslant \min(1,r+t)}(\alpha \vee \beta)$

AP5. $(P_{a,\leqslant r}\alpha \wedge P_{a,<t}\alpha) \rightarrow P_{a,<r+t}(\alpha \vee \beta),\ r + t \leqslant 1$

RPN. $\dfrac{\alpha}{P_{a,\geqslant 1}\alpha}$

RA. $\dfrac{\{\Phi_{k,\mathbf{B},\mathbf{X}}(P_{a,\geqslant r-\frac{1}{i}}\alpha) \mid i \geqslant \frac{1}{r}\}}{\Phi_{k,\mathbf{B},\mathbf{X}}(P_{a,\geqslant r}\alpha)},\ r \in (0,1]_{\mathbb{Q}}$

Strong completeness of Ax_{PTEL}

Theorem

[Soundness for Ax_{PTEL}] $\vdash \beta$ *implies* $\models \beta$.

Theorem

[Deduction theorem] If $\mathbf{T} \subset \mathbf{For}$, *then*

$$\mathbf{T}, \{\alpha\} \vdash \beta \text{ iff } \mathbf{T} \vdash \alpha \rightarrow \beta.$$

Theorem

[Strong necessitation] If $\mathbf{T} \subset \mathbf{For}$ *and* $\mathbf{T} \vdash \gamma$, *then*

1. $\bigcirc\mathbf{T} \vdash \bigcirc\gamma$,
2. $\bullet\mathbf{T} \vdash \bullet\gamma$, *and*
3. $\mathrm{K}_a\mathbf{T} \vdash \mathrm{K}_a\gamma$, *for every* $a \in \mathbf{A}$.

Strong completeness of Ax_{PTEL}

Theorem

[Lindenbaum's theorem] Every Ax_{PTEL}-consistent set of formulas $\mathbf{T}$ *can be extended to a maximal* $\mathtt{Ax}$*-consistent set* $\mathbf{T}^*$.

Theorem

[Strong completeness for Ax_{PTEL}] A set $\mathbf{T}$ *of formulas is Ax_{PTEL}-consistent iff it is satisfiable.*

Decidability of *PTEL*

- The class of all measurable *PTEL*-models is denoted by `Mod`

Theorem

The `Mod`*–satisfiability problem for* **PTEL**, **PSAT**, *is decidable.*

-

Theorem

The `Mod`*–satisfiability problem for* **PTEL** *is in 2–EXPTIME.*

-

Blockain

STEP 1 New transactions are broadcast to all nodes.

STEP 2 Each node collects new transactions into a block.

STEP 3 Each node works on finding a difficult proof-of-work for its block.

STEP 4 When a node finds a proof-of-work, it broadcasts the block to all nodes.

STEP 5 Nodes accept the block only if all transactions in it are valid and not already spent.

STEP 6 Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Fork

- Nodes always consider the longest chain (the one containing the most proofs-of-work) to be the correct one and will keep working on extending it
- If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first
- In that case, they work on the first one they received, but save the other branch in case it becomes longer
- The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

Blockain theory - BCTP

Let a, b and c denote agents from $\mathbb{A}$.

- **POW** $:= \{\text{pow}_{a,i} | a \in \mathbb{A}, i \in \mathbb{N}\}$ is a set of atomic propositions, with the intended meaning of $\text{pow}_{a,i}$ that the agent a produces a proof-of-work for round i,
- **ACC** $:= \{\text{acc}_{a,b,i} | a, b \in \mathbb{A}, i \in \mathbb{N}\}$ is a set of atomic propositions, with the intended meaning of $acc_{a,b,i}$ that the agent a accepts the proof-of-work produced for round i by the agent b,
- $e_{a,i} := \bigwedge_{b \in \mathbb{A}} (A_b \to \text{acc}_{b,a,i})$, with the intended meaning that every active agent accepts the proof-of-work produced for round i by the agent a, and
- $\text{ech}_{b,i} := \bigvee_{a \in \mathbb{A}} \text{acc}_{b,a,i}$, with the intended meaning that the agent b accepts some proof-of-work produced for round i.

Blockain theory - BCTP

AB1	$\bigvee_a A_a$	There is always at least one agent active.
AB2	$\mathsf{acc}_{b,a,i} \to \mathsf{pow}_{a,i}$	One can only accept proof-of-work that has been produced.
AB3	$\mathsf{acc}_{b,a,i} \to K_b \mathsf{acc}_{b,a,i}$	The agents know if they accept some proof-of-work.
AB4	$\mathsf{acc}_{b,a,i} \to \neg\mathsf{acc}_{b,c,i}$, for each $c \neq a$	An agent accepts at most one proof-of-work for a given round.

Blockain theory - BCTP

AB5	$\mathrm{acc}_{a,c,j} \wedge \bigcirc \mathrm{acc}_{b,a,i} \rightarrow \bigcirc \mathrm{acc}_{b,c,j}$, for $j < i$	If a accepts c's proof of work for round j and (in the next step) b accepts a's proof-of-work for a later round, then b must also accept c's proof-of-work for round j. This essentially means that if b accepts a's proof-of-work, then b accepts the whole history of a.
AB6	$A_b \wedge \bigvee_a \mathrm{pow}_{a,i} \rightarrow \mathrm{ech}_{b,i}$	If proofs-of-work for some round are produced, then each active agent must accept one of them. Note that we do not have any assumption on how an agent accepts a proof.

Blockain theory - BCTP

AB7	$\text{ech}_{a,i} \rightarrow A_a$	Only active agents can accept proofs-of-work.
AB8	$\text{ech}_{a,i+1} \rightarrow \text{ech}_{a,i}$	If an agent accepts some proof-of-work for round $i+1$, then the agent also accepts some proof-of-work for round i.

Blockain theory - BCTP

AB9	$\mathrm{ech}_{b,i} \rightarrow \bigcirc \bigvee_a \mathrm{pow}_{a,i+1}$	If an agent accepts some proof-of-work for round i, then in the next round a proof-of-work for round $i+1$ must be available.
AB10	$\neg \mathrm{ech}_{a,i} \rightarrow \neg \bigcirc \mathrm{pow}_{a,i+1}$	Only an agent that has accepted a proof-of-work for round i can create (in the next step) a proof-of-work for round $i+1$. This models the fact that a proof-of-work depends on the previously accepted history.

Blockain theory - BCTP

AB11	$\bigwedge_{a\in\mathbf{X}} \mathrm{P}_{\geqslant s_a}\mathrm{pow}_{a,i} \rightarrow \mathrm{P}_{\geqslant s}\bigwedge_{a\in\mathbf{X}}\mathrm{pow}_{a,i}$, $s=\prod_{a\in\mathbf{X}} s_a$, $\mathbf{X}\subseteq\mathbb{A}$	Necessary condition for independence of pow's.
AB12	$\bigwedge_{a\in X} \mathrm{P}_{\leqslant s_a}\mathrm{pow}_{a,i} \rightarrow \mathrm{P}_{\leqslant s}\bigwedge_{a\in\mathbf{X}}\mathrm{pow}_{a,i}$, $s=\prod_{a\in\mathbf{X}} s_a$, $\mathbf{X}\subseteq\mathbb{A}$	Necessary condition for independence of pow's.

Blockain theory - BCTP

AB13	$\mathrm{P}_{\leqslant\varepsilon}\mathsf{pow}_{a,i}$	The probability that an agent creates proof-of-work for round i is low.
AB14	$\bigvee_{a\in\mathbb{A}}\mathsf{pow}_{a,i}$	In each round at leats one agent produces proof-of-work.
AB15	$\mathrm{P}_{\geqslant s}\alpha \to \mathrm{K}_a\mathrm{P}_{\geqslant s}\alpha$	Every agent knows probabilities of runs.

Consistency: it is common knowledge among agents that that with a high probability agents achieve consensus about a long prefix of the public ledger.

- **BCTP** $\vdash P_{\geqslant 1-(1-(1-\varepsilon^2)^k)^z}(\bigvee_{j=i}^{i+z} \bigvee_{b_j \in \mathbf{A}} \bigwedge_{c \in \mathbf{A}} (A_c \to \mathrm{acc}_{c,b_j,j}))$.

Consistency: it is common knowledge among agents that that with a high probability agents achieve consensus about a long prefix of the public ledger.

- **BCTP** $\vdash \mathrm{P}_{\geqslant 1-(1-(1-\varepsilon^2)^k)^z}(\bigvee_{j=i}^{i+z} \bigvee_{b_j \in \mathbf{A}} \bigwedge_{c \in \mathbf{A}} (A_c \rightarrow \mathrm{acc}_{c,b_j,j}))$.
- Fix some position i and some integer z. Then, there is integer j between i and $i+z$ such that the probability of the follo wing event "agent b_j produces the proof-of-work (pow) and all active agents accept this pow" is equal or greater then $1-(1-(1-\varepsilon^2)^k)^z$

Consistency: it is common knowledge among agents that that with a high probability agents achieve consensus about a long prefix of the public ledger.

- $\mathbf{BCTP} \vdash \mathrm{P}_{\geqslant 1-(1-(1-\varepsilon^2)^k)^z}(\bigvee_{j=i}^{i+z} \bigvee_{b_j \in \mathbf{A}} \bigwedge_{c \in \mathbf{A}}(A_c \rightarrow \mathrm{acc}_{c,b_j,j}))$.
- Fix some position i and some integer z. Then, there is integer j between i and $i+z$ such that the probability of the follo wing event "agent b_j produces the proof-of-work (pow) and all active agents accept this pow" is equal or greater then $1-(1-(1-\varepsilon^2)^k)^z$

Theorem

$$\mathbf{BCTP} \vdash C\mathrm{P}_{\geqslant 1-(1-(1-\varepsilon^2)^k)^z}(\bigvee_{j=i}^{i+z} \bigvee_{b_j \in \mathbf{A}} \bigwedge_{c \in \mathbf{A}}(A_c \rightarrow \mathrm{acc}_{c,b_j,j})).$$